Všeobecné obchodní podmínky

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/vseobecne-obchodni-podminky

Všeobecné obchodní podmínky Kibios pro podnikatele (B2B) Smluvní podmínky pro poskytování služeb kybernetické bezpečnosti, monitoringu, správy systémů a souvisejících služeb Datum vydání: 26. 05. 2026 Účinnost: od 26. 06. 2026 Obchodní firma: Kibios s.r.o. Právní forma: společnost s ručením omezeným Sídlo: Brněnská 305/32, 664 44 Ořechov Identifikační číslo: 298 14 995 Spisová značka: C 153011 vedená u Krajského soudu v Brně Poskytovatel je podnikatelem zapsaným v obchodním rejstříku a provozuje činnost v oblasti IT a kybernetické bezpečnosti na základě příslušných živnostenských oprávnění.

1. Úvodní ustanovení

1.1. Tyto všeobecné obchodní podmínky (dále jen „VOP“) upravují vzájemná práva a povinnosti mezi poskytovatelem služeb Kibios (dále jen „poskytovatel“) a objednatelem služeb (dále jen „klient“) vznikající v souvislosti s poskytováním služeb v oblasti kybernetické bezpečnosti, bezpečnostních auditů, penetračního testování, monitoringu infrastruktury, šifrovaných záloh, správy systémů (serverů, aplikací, webových stránek) a souvisejících technických služeb (dále jen „služby“) na systémech klienta.

1.2. Tyto VOP jsou vydány v souladu se zákonem č. 89/2012 Sb., občanský zákoník (dále jen „OZ“), zákonem č. 480/2004 Sb., o některých službách informační společnosti, zákonem č. 121/2000 Sb., autorský zákon, zákonem č. 235/2004 Sb., o dani z přidané hodnoty, zákonem č. 40/2009 Sb., trestní zákoník, zákonem č. 99/1963 Sb., občanský soudní řád, zákonem č. 264/2025 Sb., o kybernetické bezpečnosti, a Nařízeními EU (GDPR, DORA, Data Act, AI Act, Cyber Resilience Act).

1.3. VOP jsou nedílnou součástí každé smlouvy uzavřené mezi poskytovatelem a klientem (dále jen „Smlouva“), není-li smluvně dohodnuto jinak. Odchylná ustanovení Smlouvy mají přednost před zněním VOP.

1.4. Tyto VOP se vztahují výhradně na vztahy mezi podnikateli (B2B). Poskytovatel poskytuje služby pouze klientům, kteří jednají v rámci své podnikatelské činnosti nebo výkonu povolání. Ustanovení o spotřebitelích dle § 1810 a násl. OZ a zákona č.

634/1992 Sb., o ochraně spotřebitele, se na Smlouvu nepoužijí.

2. Vymezení pojmů

„Služba“ – jakákoli z činností nabízených poskytovatelem (bezpečnostní audit, analýza zranitelností, oprava zranitelností, penetrační testování, kompletní správa, monitoring, šifrované zálohy, logování událostí, správa systémů klienta včetně serverů a webových aplikací, voicemail/IVR služby aj.). „Systémy klienta“ – informační systémy, aplikace, servery, webové stránky, databáze, síťové prvky a další IT prostředky, které klient vlastní, spravuje nebo provozuje a na kterých jsou poskytovatelem poskytovány služby dle Smlouvy. „Monitorované systémy“ – systémy

klienta, které jsou výslovně uvedeny ve Smlouvě nebo její příloze jako systémy pod monitorováním poskytovatele (např. systémy zahrnuté do SLA, logování, alertingu). „Audit“ – analýza zranitelností a bezpečnostní kontrola systémů klienta dle dohodnuté metodiky (např. OWASP ASVS, ISO/IEC 27001 přílohy A, NIST CSF 2.0).

„Penetrační test“ – řízený pokus o průnik do systémů klienta provedený s jeho prokazatelným písemným souhlasem (Rules of Engagement – RoE).

„Kompletní správa“ – paušální služba zahrnující kontinuální monitoring, aktualizace, zálohy, logování, incident response a podporu v rozsahu sjednaném ve Smlouvě.

„SLA“ – Service Level Agreement, garantovaná úroveň dostupnosti služeb a reakční čas incidentů na monitorovaných systémech. „Incident“ – událost, která má nebo může mít dopad na bezpečnost, dostupnost, integritu nebo důvěrnost systémů klienta; ve smyslu zákona č. 264/2025 Sb., o kybernetické bezpečnosti. „Závažný incident“ – incident s významným dopadem dle § 6 zákona č. 264/2025 Sb.

„Osobní údaje“ – informace ve smyslu čl. 4 odst. 1 GDPR. „Subjekt údajů“ – fyzická osoba, jejíž osobní údaje jsou zpracovávány.

3. Předmět služeb a způsob plnění

3.1. Poskytovatel se zavazuje pro klienta provádět služby v rozsahu sjednaném ve Smlouvě, cenové nabídce, SOW nebo online objednávce, které odkazují na tyto VOP.

3.2. Před zahájením auditu, penetračního testování nebo jakéhokoli aktivního zásahu do systémů klienta poskytovatel a klient dohodnou zejména:

- cíle a rozsah testování (in-scope / out-of-scope, IP rozsahy, domény);
- časový rámec a okno pro provedení;
- kontaktní osoby a eskalační kanály;
- pravidla pro nakládání s nalezenými zranitelnostmi (responsible disclosure);
- Rules of Engagement (RoE), které mohou být klientem odsouhlaseny elektronicky prostřednictvím klientského portálu nebo dashboardu Kibios (např. zaškrtnutím souhlasu a potvrzením).

3.3. Poskytovatel provádí penetrační testy a jiné aktivní bezpečnostní testování systémů klienta pouze tehdy, pokud klient elektronicky odsouhlasil RoE prostřednictvím klientského portálu nebo dashboardu Kibios, případně jiným prokazatelným elektronickým způsobem. Klient bere na vědomí, že bez tohoto elektronického souhlasu penetrační testání neproběhne, neboť by mohlo být v rozporu se zákonem (§ 230 trestního zákoníku – neoprávněný přístup k počítačovému systému).

3.4. Poskytovatel se zavazuje provádět sjednané služby s odbornou péčí podle praxe v oblasti kybernetické bezpečnosti, správy IT systémů a webových aplikací.

3.5. U služeb zahrnujících aktualizace systémů, aplikací nebo webových stránek poskytovatel odpovídá za:

- aplikaci aktualizací na určené systémy klienta;
- základní funkční kontrolu po aktualizaci (dostupnost, klíčové funkcionality monitorovaných systémů);
- vedení záznamů o provedených aktualizacích.

3.6. Výstupy auditů a penetračních testů (reporty) mohou obsahovat doporučená bezpečnostní opatření; za jejich implementaci odpovídá klient, není-li sjednáno, že ji zajišťuje poskytovatel.

3.7. Klient se zavazuje informovat poskytovatele předem o významných změnách na systémech klienta v rozsahu služeb, zejména:

- instalace nových pluginů / modulů do webových aplikací;
- aktualizace nebo výměna aplikací, knihoven, frameworků;
- změny konfigurace serverů, databází, bezpečnostních politik nebo přístupových práv.

3.8. Pokud klient provede takové změny bez informování poskytovatele nebo bez jeho součinnosti, poskytovatel neodpovídá za škody vzniklé v důsledku těchto změn, není-li ve Smlouvě dohodnuto jinak.

3.9. Klient je povinen:

- zajistit poskytovateli potřebné přístupy k systémům klienta;
- aktualizovat kontaktní osoby pro technickou/provozní komunikaci;
- zajistit, aby osoby s administrátorskými oprávněními byly seznámeny s těmito VOP.

3A. Smluvní dokumentace Kibios

3A.1. Vedle těchto VOP využívá poskytovatel při poskytování služeb následující dokumenty (dále jen „Bezpečnostní dokumentace Kibios“):

- Master Service Agreement (MSA);
- Service Level Agreement (SLA);
- Data Processing Agreement (DPA);
- Acceptable Use Policy (AUP);
- Incident Response Policy;
- Backup Policy;
- Vulnerability Disclosure Policy (VDP);
- Responsible Disclosure Policy;
- Rules of Engagement (RoE);
- Statement of Work (SOW);
- Change Management Policy;
- Business Continuity Plan (BCP);
- Disaster Recovery Plan (DRP);
- Information Security Policy;
- Asset Management Policy;
- Access Control Policy;
- Password Policy;
- Remote Access Policy;
- Logging & Monitoring Policy;
- Secure Development Policy;

- Data Retention Policy;
- Privacy Policy;
- Cookie Policy.

3A.2. Vybrané dokumenty (MSA, SLA, DPA, AUP, RoE, SOW) tvoří součást Smlouvy jako přílohy nebo na ně Smlouva výslovně odkazuje. Ostatní dokumenty jsou interní nebo zveřejněné politiky poskytovatele upravující technické a organizační aspekty služeb.

3A.3. Klient bere na vědomí, že technické detaily (parametry SLA, incident response, zálohování, logging, secure development, data retention) jsou upraveny v Bezpečnostní dokumentaci Kibios. Klient může kdykoli požádat o aktuální verzi dokumentů, které jsou pro něj relevantní.

4. Uzavření smlouvy a online akceptace VOP

4.1. Smlouva mezi poskytovatelem a klientem vzniká:

- podpisem MSA nebo SOW;
- písemnou objednávkou / akceptací cenové nabídky (e-mail, elektronický podpis);
- nebo online objednávkou / registrací na webu Kibios, kde je klient informován
  - VOP a má možnost se s nimi seznámit.

4.2. Klient bere na vědomí, že odesláním objednávky, registrací, úhradou faktury nebo využitím služeb Kibios (včetně free testů) akceptuje tyto VOP, pokud byl o jejich existenci informován a měl možnost se s nimi seznámit.

4.3. Oboustranně potvrzená e-mailová komunikace mezi oprávněnými osobami stran se považuje za písemnou formu ve smyslu § 562 odst. 1 OZ.

4.4. Klient prohlašuje, že je vlastníkem systémů klienta nebo má oprávnění vlastníka k jejich testování, správě a monitoringu.

4.5. Klient bere na vědomí, že určitá dílčí ujednání (např. RoE pro penetrační testy) mohou být odsouhlasována výhradně elektronicky prostřednictvím klientského portálu nebo dashboardu Kibios. Za odsouhlasené se považují okamžikem, kdy oprávněná osoba klienta v příslušném rozhraní:

- potvrdí, že údaje v RoE odpovídají skutečnosti (scope, čas, kontaktní osoby apod.), a
- expressis verbis (např. zaškrtnutím políčka „Souhlasím s RoE“ a stiskem tlačítka „Potvrdit“) vyjádří souhlas.

5. Cena a platební podmínky

5.1. Ceny služeb jsou stanoveny v SOW, cenové nabídce, ceníku nebo online nabídce poskytovatele. Není-li uvedeno jinak, jsou ceny v Kč bez DPH; DPH dle zákona č.

235/2004 Sb.

5.2. Jednorázové služby (audit, jednorázová oprava, konzultace) – faktura splatná do 14 dnů od vystavení, poskytovatel může požadovat zálohu až 50 % ceny před zahájením.

5.3. Paušální služby (balíčky Základní jistota, Monitoring a aktualizace, Audity a opravy, Aktivní obrana, Kompletní správa, Pen-testy a dohled) – fakturovány předem za zvolené předplacené období (1, 3, 6, 9, 12, 18, 24 měsíců); splatnost 14 dnů.

5.4. V případě prodlení s úhradou je poskytovatel oprávněn účtovat zákonný úrok z prodlení. Při prodlení delším než 30 dnů může poskytovatel po upozornění (min. 7 dní předem) služby dočasně pozastavit.

5.5. Faktury jsou zasílány elektronicky na e-mail klienta uvedený ve Smlouvě; klient s tím souhlasí.

6. Doba trvání služeb a ukončení

6.1. Jednorázové služby končí splněním (dokončením).

6.2. Paušální služby se sjednávají na předplacené období; Smlouva je závazná po celé období, výpověď je účinná nejdříve k jeho konci, pokud není smluvně dohodnuto jinak. Předplacené částky se nevracejí, nejde-li o ukončení z důvodu podstatného porušení Smlouvy nebo zákonného odstoupení.

6.3. Strany mohou od Smlouvy odstoupit s okamžitou účinností v případě podstatného porušení smluvních povinností druhou stranou (§ 2002 OZ).

6.4. Ustanovení o spotřebitelském odstoupení při distančním uzavření smlouvy se nepoužijí (B2B režim).

7. SLA a dostupnost služeb

7.1. Konkrétní úrovně SLA (dostupnost, reakční časy, doby opravy) jsou stanoveny v SLA příloze nebo Smlouvě. Typicky se rozlišuje: Priorita P1 – kritický incident: úplný výpadek služby, ransomware, kompromitace administrátorského účtu, aktivní útok s dopadem na produkční systémy klienta.

Priorita P2 – vysoká priorita: významné omezení provozu, výpadek části systému, závažná zranitelnost bez aktuálního exploitu. Priorita P3 – střední priorita: chyba aplikace, nefunkční modul, omezená funkcionalita bez zásadního dopadu na bezpečnost. Priorita P4 – nízká priorita: kosmetické chyby, nastavení, konzultace.

7.2. SLA dostupnost se počítá měsíčně pro monitorované systémy a nezahrnuje:

- plánované odstávky (max. 4 h/měsíc, oznámené min. 48 h předem, v okně 22:00–05:00 CET);
- vyšší moc;
- výpadky způsobené třetími stranami mimo kontrolu poskytovatele (konektivita, datacentra, DNS);
- zásahy do systémů klienta ze strany klienta nebo jeho dodavatelů bez souhlasu poskytovatele.

7.3. Standardní maintenance window: sobota 22:00–04:00 nebo neděle 00:00–05:00 CET. V případě kritické zranitelnosti (CVSS 9,0–10 nebo aktivní exploit) je poskytovatel oprávněn provést nouzovou údržbu mimo toto okno a bez standardního oznamovacího termínu, pokud je to nezbytné k ochraně systémů klienta.

7.4. SLA se vztahuje pouze na služby poskytovatele a výslovně uvedené monitorované systémy.

7.5. Nedodržení SLA zakládá nárok na slevu z paušálu dle SLA přílohy; pokud nedodržení souvisí se změnou na systémech klienta provedenou bez informování poskytovatele, nárok na slevu nevzniká.

8. Odpovědnost za škodu

8.1. Poskytovatel poskytuje služby s odbornou péčí v souladu se Smlouvou, VOP a standardy (OWASP, ISO/IEC 27001, NIST CSF). Odpovídá za škodu vzniklou porušením jeho povinností.

8.2. Poskytovatel nezajišťuje absolutní bezpečnost; služby snižují riziko, nikoli je eliminují.

8.3. Poskytovatel neodpovídá za samotný vznik kybernetického útoku ani jeho úspěšnost, pokud plnil své povinnosti. Neodpovídá zejména za škody z:

- sofistikovaného útoku (APT, státní aktér), zero-day exploitu;
- útoku realizovaného uživatelským chováním (phishing, škodlivé přílohy, instalace malwaru);
- útoků na systémy, které nejsou v rozsahu služeb.

8.4. Poskytovatel neodpovídá za škody způsobené:

- změnou konfigurace, zabezpečení nebo instalací pluginů ze strany klienta nebo třetí osoby;
- zásahy, které logy přisuzují klientovi nebo třetí osobě mimo kontrolu poskytovatele;
- neprovedením doporučených bezpečnostních opatření;
- událostmi vyšší moci (cloud/datacenter outage, IX/DNS/BGP incidenty, válka, státní zásahy, rozsáhlý blackout).

8.5. Poskytovatel neodpovídá za nepřímé škody, ušlý zisk, ztrátu dat či poškození dobrého jména, ledaže by byly způsobeny úmyslně nebo z hrubé nedbalosti.

8.6. Maximální výše náhrady škody je omezena částkou odpovídající celkové ceně služeb zaplacené klientem poskytovateli za 12 měsíců před vznikem škody (u jednorázových služeb cenou dané služby), pokud škoda nebyla způsobena úmyslně nebo hrubou nedbalostí.

8.7. Pro posouzení incidentu jsou rozhodující logy a monitorovací záznamy poskytovatele a klienta.

8.8. Poskytovatel má sjednané profesní pojištění odpovědnosti.

9. Mlčenlivost

9.1. Strany se zavazují k mlčenlivosti o důvěrných informacích druhé strany.

9.2. Mlčenlivost trvá 5 let po skončení Smlouvy; u obchodního tajemství a osobních údajů bez časového omezení.

9.3. Výstupy z auditů a pen-testů jsou přísně důvěrné; sdílení je možné jen se souhlasem klienta nebo v zákonem stanovených případech.

10. Kybernetická bezpečnost a incident response

10.1. Poskytovatel se řídí zákonem č. 264/2025 Sb. a metodikami NÚKIB.

10.2. Klient, který spadá pod zákon o kybernetické bezpečnosti, nese vlastní zákonné povinnosti; poskytovatel poskytuje technické plnění dle Smlouvy.

10.3. Závažný incident v monitorovaných systémech – poskytovatel informuje klienta bez zbytečného odkladu, nejpozději do 4 hodin od zjištění.

10.4. Post-mortem report bude předán do 30 dnů od uzavření incidentu.

10.5. Klient informuje poskytovatele o podezřelých aktivitách nebo kompromitaci.

10.6. Poskytovatel doporučí nápravná opatření; za jejich implementaci odpovídá klient, není-li sjednáno jinak.

11. Responsible / Coordinated Disclosure

11.1. Poskytovatel uplatňuje coordinated vulnerability disclosure vůči vendorům třetích stran.

11.2. Vendor a klient jsou informováni; po přiměřené lhůtě může být zranitelnost zveřejněna v anonymizované formě, pokud tím není narušena bezpečnost klienta.

12. DORA

12.1. Pokud je klient finanční institucí dle Nařízení (EU) 2022/2554 (DORA), poskytovatel plní roli ICT třetí strany v souladu s DORA.

12.2. Klient odpovídá za zápis služeb Kibios do svého DORA registru.

13. Ochrana osobních údajů

13.1. Zpracování osobních údajů se řídí samostatným DPA, který je součástí Smlouvy.

13.2. Pokud poskytovatel vystupuje jako zpracovatel dle čl. 28 GDPR, strany uzavírají DPA.

13.3. Předávání údajů mimo EHP je možné jen v souladu s GDPR.

14. Duševní vlastnictví

14.1. Výstupy poskytovatele (reporty, skripty, konfigurace, dashboardy) zůstávají jeho duševním vlastnictvím; klient má nevýhradní, nepřenosnou licenci pro vlastní vnitřní potřebu na dobu trvání Smlouvy + 3 roky.

14.2. Klient nesmí výstupy poskytovat třetím osobám ani je komerčně využívat bez souhlasu poskytovatele (s výjimkou poradců vázaných mlčenlivostí).

14.3. Open-source nástroje se řídí vlastními licencemi.

15. Acceptable Use a Abuse Process

15.1. Klient nesmí prostřednictvím služeb Kibios provozovat spam, phishing, šíření malwaru, C2 servery, botnety, cryptomining, DDoS útoky ani jiné nezákonné či neetické aktivity.

15.2. Při oznámení abuse poskytovatel informuje klienta, který je povinen do 24 hodin reagovat a přijmout nápravná opatření.

15.3. Pokud klient nereaguje nebo nápravu neprovede, poskytovatel je oprávněn službu dočasně pozastavit.

16. Penetrační testy a důkazní materiály

16.1. Není-li sjednáno jinak, pen-testy nezahrnují DoS, ransomware, destruktivní payload, mazání dat, trvalou persistenci, cryptomining ani jiné zásahy způsobující ztrátu dat či provozu.

16.2. Poskytovatel vede základní chain of custody u důkazních materiálů (kdo, kdy, jak, SHA256 hash).

16.3. Citlivá data získaná v rámci testu/incidentu (databáze, hesla, tokeny) jsou použita jen jako důkaz (screenshot/hash) a po skončení testu/incidentu bezpečně smazána.

17. Reklamace

17.1. Klient reklamuje vady díla bez zbytečného odkladu, nejpozději do 30 dnů od zjištění, na info@kibios.com nebo na adresu sídla poskytovatele.

17.2. Reklamace musí obsahovat identifikaci klienta, službu, popis vady a požadovaný způsob řešení.

17.3. Poskytovatel vady odstraní v přiměřené lhůtě, obvykle do 14 dnů; lhůta může být dohodou prodloužena.

18. Řešení sporů

18.1. Strany se pokusí spory řešit smírně.

18.2. Věcně a místně příslušný je soud v České republice; strany sjednávají místní příslušnost soudu dle sídla poskytovatele, není-li to v rozporu se zákonem.

19. Závěrečná ustanovení

19.1. Tyto VOP a vztahy mezi poskytovatelem a klientem se řídí českým právem, zejména OZ.

19.2. Neplatnost nebo neúčinnost jednotlivého ustanovení nemá vliv na platnost ostatních ustanovení; neplatné ustanovení bude nahrazeno ustanovením s obdobným smyslem.

19.3. Poskytovatel je oprávněn VOP měnit; klient bude informován min. 30 dní před účinností nové verze (e-mail, portál). Pokud nesouhlasí, může Smlouvu vypovědět ke dni účinnosti nové verze.

19.4. Klient prohlašuje, že se s VOP seznámil, porozuměl jim a souhlasí s nimi v plném rozsahu.

19.5. VOP jsou vyhotoveny v českém jazyce; v případě překladu je rozhodující české znění.

20. Kontaktní údaje

Poskytovatel: Kibios s.r.o. Sídlo: Brněnská 305/32, 664 44 Ořechov E-mail (obecný kontakt): info@kibios.com E-mail (reklamace / právní): info@kibios.com E-mail (incident response 24/7): security@kibios.com