Pravidla pro nahlašování bezpečnostních zranitelností

Provozovatel: LexAI Technologies, s.r.o., IČO: 23589825, se sídlem Školská 660/3, Praha 1 — Nové Město, 110 00 Praha 1

Účinnost: 5. května 2026

Kontakt pro bezpečnostní hlášení: support@lexaitechnologies.com

1. Úvod

Bezpečnost platformy LexAI je pro nás zásadní. LexAI je postaveno na principu zero-knowledge architektury a důvěra uživatelů v ochranu jejich dat je základem našeho produktu. Pokud jste objevili bezpečnostní zranitelnost v naší platformě, oceníme, pokud nám ji nahlásíte v souladu s těmito pravidly.

Důležité upozornění: LexAI v tuto chvíli **neprovozuje veřejný bug bounty program** a za nahlášené zranitelnosti **neposkytuje finanční odměny**. Aktivní bezpečnostní testování (penetrační testy, fuzzing, scanning, atd.) bez našeho předchozího písemného souhlasu **není povoleno** — viz článek 6.2(b) Podmínek používání. Tato pravidla se vztahují na případy, kdy zranitelnost objevíte při běžném používání platformy nebo v rámci samostatného bezpečnostního výzkumu, který neporušuje naše Podmínky používání.

2. Rozsah

2.1 Co spadá do rozsahu

Hlášení v rámci těchto pravidel přijímáme pro:

- platformu LexAI dostupnou na www.lexaitechnologies.app
- webové stránky www.lexaitechnologies.com
- API a serverless funkce provozované pod doménou LexAI
- klientskou (browser-side) implementaci kryptografických operací

2.2 Co do rozsahu nespadá

Hlášení nepřijímáme pro:

- zranitelnosti v systémech třetích stran (Anthropic, Supabase, Vercel, Stripe, SendGrid, Hetzner, Qdrant, SerpAPI, Brave Search, IPInfo) — tyto nahlaste přímo dotčenému poskytovateli
- problémy nalezené prostřednictvím testů, které porušily článek 6.2(b) Podmínek používání

- sociální inženýrství našich zaměstnanců, dodavatelů nebo uživatelů
- fyzické útoky proti naší infrastruktuře nebo kancelářím
- denial-of-service (DoS/DDoS) útoky a testy
- zranitelnosti vyžadující kompromitaci uživatelského zařízení útočníkem (out-of-scope threat model)
- problémy způsobené zastaralými verzemi prohlížečů, které neodpovídají našim minimálním technickým požadavkům
- best-practice doporučení bez konkrétního exploitable scénáře (např. „chybí HTTP hlavička X")

3. Co očekáváme od vás

Pokud nám hlásíte zranitelnost, žádáme vás, abyste:

1. **Nahlásili nález soukromě** na security@lexaitechnologies.com a nezveřejňovali jej před tím, než jej opravíme nebo se s vámi dohodneme na koordinovaném zveřejnění.
2. **Nepřistupovali k datům jiných uživatelů**, neměnili je ani je neexfiltrovali. Pokud při testování omylem získáte přístup k cizím datům, okamžitě ukončete testování a uveďte to v hlášení.
3. **Neprováděli aktivní testování ve velkém rozsahu** (automatizovaný scanning, fuzzing, brute-force, DoS). Pokud pro ověření nálezu potřebujete provést konkrétní omezený test, vyžádejte si nejprve náš souhlas.
4. **Nezneužívali zranitelnost** nad rámec nezbytný k jejímu prokázání (proof of concept).
5. **Poskytli nám přiměřený čas na opravu** předtím, než informace zveřejníte. Standardně se řídíme principem koordinovaného zveřejnění s lhůtou 90 dnů od potvrzení hlášení; u kritických zranitelností se tato lhůta může prodloužit po vzájemné dohodě.
6. **Dodržovali platné právní předpisy** během testování i hlášení.

4. Co slibujeme my

Pokud postupujete v souladu s těmito pravidly:

1. **Bezpečný přístav:** Nebudeme proti vám podnikat právní kroky a nebudeme vyžadovat trestní stíhání za bezpečnostní výzkum prováděný v dobré víře a v souladu s těmito pravidly. Tento závazek se vztahuje pouze na vaše jednání vůči LexAI; nemůžeme vás zbavit odpovědnosti vůči třetím stranám ani vůči orgánům veřejné moci. **Posouzení toho, zda hlášení a postup výzkumníka splňují podmínky těchto pravidel a zakládají dobrou víru, provádí LexAI.**
2. **Reakce v rozumném čase:**
   - **Potvrzení přijetí hlášení:** do 3 pracovních dnů
   - **První věcné posouzení:** do 14 dnů od potvrzení
   - **Informace o průběhu opravy:** v rozumných intervalech až do uzavření případu
3. **Transparentnost:** Budeme s vámi komunikovat o tom, jak hlášení vyhodnocujeme a kdy plánujeme opravu.
4. **Uznání (volitelné):** Pokud si to budete přát, uvedeme vás v našem seznamu výzkumníků, kteří přispěli k bezpečnosti LexAI. Pokud preferujete anonymitu, plně to respektujeme.

5. Jak nahlásit zranitelnost

Hlášení odešlete na support@lexaitechnologies.com s předmětem začínajícím **„[SECURITY]"**, abychom mohli hlášení rychle identifikovat a eskalovat. Hlášení by mělo obsahovat:

- **Popis zranitelnosti** — co jste objevili, jaký dopad to může mít
- **Kroky k reprodukci** — co nejpodrobnější postup, ideálně včetně request/response, screenshotů nebo videa
- **Dotčená komponenta** — URL, endpoint, funkcionalita
- **Vaše hodnocení závažnosti** (volitelné) — např. dle CVSS
- **Návrh na opravu** (volitelné) — pokud máte
- **Vaše kontaktní údaje** a preferovaný jazyk komunikace (cs/en)

5.1 Šifrované hlášení

Pro citlivá hlášení (zejména zranitelnosti v autentizační nebo kryptografické vrstvě) doporučujeme komunikaci šifrovat. PGP klíč pro šifrovanou komunikaci poskytneme na vyžádání — uveďte tento požadavek v úvodním e-mailu a zašleme vám veřejný klíč zpět.

6. Hodnocení a klasifikace zranitelností

Pro hodnocení závažnosti používáme standard CVSS v3.1. Prioritu opravy stanovujeme zejména podle:

- dopadu na důvěrnost dat uživatelů (zejména prolomení zero-knowledge architektury)
- dopadu na integritu a dostupnost služby
- možnosti zneužití bez interakce uživatele
- rozsahu potenciálně dotčených uživatelů

Zranitelnosti, které by mohly vést k prolomení zero-knowledge architektury (tedy získání nešifrovaného přístupu k uživatelským konverzacím nebo dokumentům), považujeme za nejvyšší prioritu.

7. Co tato pravidla nepředstavují

Tato pravidla:

- **nezakládají smluvní vztah** mezi vámi a LexAI
- **nezakládají nárok** na odměnu, kompenzaci nebo jakékoli plnění ze strany LexAI
- **neopravňují** vás k aktivnímu testování naší platformy bez výslovného souhlasu
- **nenahrazují** Podmínky používání ani Zásady ochrany osobních údajů, které platí v plném rozsahu

8. Změny pravidel

LexAI si vyhrazuje právo tato pravidla kdykoli aktualizovat. Aktuální verze je vždy dostupná na https://www.lexaitechnologies.com/security. Změny nemají zpětný účinek na hlášení podaná

před účinností nové verze.

9. Kontakt

LexAI Technologies, s.r.o. Školská 660/3, Praha 1 — Nové Město, 110 00 Praha 1 E-mail: support@lexaitechnologies.com Web: www.lexaitechnologies.com

Verze 1.0 — účinná od 5. května 2026