# Vulnerability Disclosure Policy

**Operator:** LexAI Technologies, s.r.o., Company ID (IČO): 23589825, registered office: Školská 660/3, Praha 1 — Nové Město, 110 00 Praha 1

**Effective date:** 5 May 2026

**Contact for security reports:** support@lexaitechnologies.com

## 1. Introduction

Security of the LexAI platform is fundamental to us. LexAI is built on a zero-knowledge architecture, and user trust in the protection of their data is central to our product. If you have discovered a security vulnerability in our platform, we appreciate you reporting it in accordance with this policy.

**Important notice:** LexAI does **not currently operate a public bug bounty program** and does **not offer monetary rewards** for reported vulnerabilities. Active security testing (penetration testing, fuzzing, scanning, etc.) without our prior written consent is **not permitted** — see Section 6.2(b) of our Terms of Use. This policy applies in cases where you discover a vulnerability through normal use of the platform or through independent security research that does not violate our Terms of Use.

## 2. Scope

### 2.1 In Scope

We accept reports under this policy for:

- the LexAI platform available at www.lexaitechnologies.app
- the website www.lexaitechnologies.com
- APIs and serverless functions operated under LexAI domains
- the client-side (browser) implementation of cryptographic operations

### 2.2 Out of Scope

We do not accept reports for:

- vulnerabilities in third-party systems (Anthropic, Supabase, Vercel, Stripe, SendGrid, Hetzner, Qdrant, SerpAPI, Brave Search, IPInfo) — please report these directly to the relevant provider
- issues found through testing that violated Section 6.2(b) of our Terms of Use
- social engineering of our employees, contractors, or users
- physical attacks against our infrastructure or offices
- denial-of-service (DoS/DDoS) attacks and tests

- vulnerabilities requiring attacker-controlled compromise of a user's device (out-of-scope threat model)
- issues caused by outdated browser versions that do not meet our minimum technical requirements
- best-practice recommendations without a concrete exploitable scenario (e.g. "missing HTTP header X")

## 3. What We Expect From You

If you report a vulnerability to us, we ask that you:

1. **Report the finding privately** to support@lexaitechnologies.com and do not disclose it publicly before we have remediated it or agreed with you on coordinated disclosure.
2. **Do not access other users' data**, modify it, or exfiltrate it. If during testing you accidentally gain access to data belonging to others, stop testing immediately and disclose this in your report.
3. **Do not conduct large-scale active testing** (automated scanning, fuzzing, brute-force, DoS). If you need to perform a specific limited test to verify a finding, request our consent first.
4. **Do not exploit the vulnerability** beyond what is necessary to demonstrate it (proof of concept).
5. **Allow us reasonable time to remediate** before publicly disclosing. We follow the principle of coordinated disclosure with a standard 90-day window from confirmation of the report; for critical vulnerabilities, this period may be extended by mutual agreement.
6. **Comply with applicable law** during testing and reporting.

## 4. What We Promise

If you proceed in accordance with this policy:

1. **Safe harbor:** We will not pursue legal action against you and will not seek criminal prosecution for security research conducted in good faith and in compliance with this policy. This commitment applies only to your conduct vis-à-vis LexAI; we cannot release you from liability towards third parties or public authorities. **Whether a report and the researcher's conduct meet the conditions of this policy and constitute good faith is determined by LexAI.**
2. **Reasonable response times:**
   - **Acknowledgement of receipt:** within 3 business days
   - **Initial substantive assessment:** within 14 days of acknowledgement
   - **Updates on remediation progress:** at reasonable intervals until the case is closed
3. **Transparency:** We will communicate with you regarding how we evaluate the report and when remediation is planned.
4. **Acknowledgement (optional):** If you wish, we will list you in our acknowledgements of researchers who have contributed to LexAI's security. If you prefer to remain anonymous, we will fully respect that.

## 5. How to Report a Vulnerability

Submit reports to support@lexaitechnologies.com with the subject line beginning **"[SECURITY]"** so that we can quickly identify and escalate the report. Reports should include:

- **Description of the vulnerability** — what you discovered and what impact it may have
- **Steps to reproduce** — as detailed as possible, ideally including request/response data, screenshots, or video
- **Affected component** — URL, endpoint, functionality
- **Your severity assessment** (optional) — e.g. using CVSS
- **Proposed remediation** (optional) — if you have one
- **Your contact details** and preferred language of communication (cs/en)

### 5.1 Encrypted Reports

For sensitive reports (in particular vulnerabilities in the authentication or cryptographic layer), we recommend encrypting communications. A PGP key for encrypted communication is available on request — include this request in your initial email and we will return the public key to you.

## 6. Vulnerability Assessment and Classification

We use the CVSS v3.1 standard to assess severity. Remediation priority is determined primarily by:

- impact on the confidentiality of user data (in particular any compromise of the zero-knowledge architecture)
- impact on the integrity and availability of the service
- ease of exploitation without user interaction
- scope of potentially affected users

Vulnerabilities that could lead to a compromise of the zero-knowledge architecture (i.e. obtaining unencrypted access to user conversations or documents) are treated as the highest priority.

## 7. What This Policy Does Not Constitute

This policy:

- **does not establish a contractual relationship** between you and LexAI
- **does not create any entitlement** to a reward, compensation, or any other benefit from LexAI
- **does not authorise** you to actively test our platform without our explicit consent
- **does not replace** the Terms of Use or Privacy Policy, which remain in full force and effect

## 8. Changes to This Policy

LexAI reserves the right to update this policy at any time. The current version is always available at https://www.lexaitechnologies.com/cs/vulnerability-disclosure/. Changes do not

have retroactive effect on reports submitted prior to the effective date of the new version.

## 9. Contact

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

*Version 1.0 — effective from 5 May 2026*