Security & Disclosure

Effective 22 Nov 2026 Version 1.0 For everyone

The short version

- Traffic is encrypted in transit; Electron Hub is not end-to-end encrypted.
- Treat API keys like passwords and revoke any key you think is exposed.
- Report vulnerabilities to support@electronhub.ai; we won't pursue good-faith research.

This summary helps you find your way. The full text below is what applies.

1. How we protect the Service

- All connections to Electron Hub use TLS encryption in transit.
- Session tokens are stored as hashes. OAuth tokens for MCP servers are stored encrypted. Keys you bring for other services (BYOK) are used per request and not stored.
- Access to production systems and data is limited to the people who need it.
- We use Cloudflare's network protection, rate limits and abuse detection.

Electron Hub is not end-to-end encrypted. Your requests are decrypted on our servers so they can be routed and sent to the Model Provider that processes them, as described in the Privacy Policy.

2. Keeping your account safe

- Treat every API key like a password. Do not put keys in client-side code, public repositories or shared documents.
- Use proxy keys with spending caps for your apps and for colleagues in your own organisation, instead of sharing your master key (Terms Section 4.3).
- If a key may be exposed, revoke it in the Console straight away. You are responsible for usage until a key is revoked (Terms Section 4.2).

- Your chats, files and API key are stored in your browser. Protect your device and browser profile, and sign out on shared computers.

---

3. Reporting a vulnerability

Email support@electronhub.ai with the subject "Security" and include a description, the steps to reproduce, the affected URL or endpoint, and the impact you expect. We aim to acknowledge reports within 3 business days.

Please: test only against your own account and data; stop and report as soon as you can show the issue; give us a reasonable time to fix it before you disclose it publicly.

Please don't: access, change or delete other users' data; run denial-of-service, spam or social-engineering tests; use automated scanners that generate heavy traffic; or use a vulnerability beyond what is needed to show it.

If you follow these rules in good faith, we will not take legal action against you for your research and will work with you to understand and fix the issue. We do not currently run a paid bug bounty.

---

4. Incidents

If a security incident affects your personal data in a way that puts your rights at risk, we will tell you without undue delay and notify regulators where the law requires, as described in the Privacy Policy.