

Responsible Disclosure Policy

How to report a vulnerability, what we commit to, and what we ask of researchers.

Version 1.0 · Last reviewed 22 October 2026 · Owner: Security Lead, security@etropo.com · Current version at <https://trust.etropo.com/resources/responsible-disclosure-policy>

1. Reporting a vulnerability

If you believe you have found a security vulnerability in Etropo, email security@etropo.com with:

- the steps to reproduce it, with URLs, requests or a proof of concept;
- what you were able to see or do;
- your contact details, if you want to be credited or kept informed.

Please do not report vulnerabilities through support chat, social media or public issue trackers.

2. What we commit to

- Acknowledge your report within **48 hours**.
- Tell you within 7 days whether we have confirmed the issue and how serious we rate it.
- Keep you updated while we fix it, and tell you when it is fixed.
- Fix confirmed issues within the targets in the Secure Development Policy: 48 hours for critical, 7 days for high, 30 days for medium.
- Credit you publicly, with your consent, once the issue is fixed.
- Not take legal action against researchers who follow this policy.

Etropo does not currently run a paid bounty programme.

3. What we ask

- Give us a reasonable time to fix the issue before you disclose it publicly. We aim to agree a date with you.
- Do not access, change or delete data that is not yours. If you reach another customer's data, stop and report it.
- Do not degrade the service: no denial-of-service, no automated scanning at a rate that affects other users, no social engineering of Etropo personnel or customers.
- Use only accounts you created for testing.
- Do not demand payment in exchange for the report.

4. Scope

- **In scope:** app.etropo.com, api endpoints under it, the MCP server, the Slack, Teams and HubSpot integrations, www.etropo.com and trust.etropo.com.
- **Out of scope:** the platforms Etropo runs on (Vercel, Supabase, Stripe and the other vendors on the Subprocessors page), which have their own programmes; findings that need physical access or a compromised device; reports from automated scanners without a demonstrated impact; missing best-practice headers without an exploit.

5. Safe harbour

Research conducted in line with this policy is authorised. We will not pursue civil or criminal action for it and will say so to any third party that asks.

Version 1.0, October 2026.

This PDF is a snapshot. The page at <https://trust.etropo.com/resources/responsible-disclosure-policy> is the current version.