

Security and Responsible Disclosure

How we protect your services and data, and how to report a security vulnerability to us.

Policies Version 1.0 Effective 20 October 2026 Last updated 20 October 2026

In short

- We use encryption, access controls, monitoring, regular updates and two-step sign-in.
- Found a vulnerability? Email hello@pricehq.tech with "Security" in the subject.
- Test in good faith, don't access other people's data, and give us time to fix it; we won't take legal action against you.

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

This policy explains how we keep our services secure and how to tell us about a security problem.

1. How we protect your services

- 1.1 Connections to our website, client area, control panel and email use encryption (HTTPS and TLS).
- 1.2 Staff systems require two-step sign-in, and access is limited to people who need it.
- 1.3 Our servers are kept updated, monitored around the clock, protected by firewalls and intrusion blocking, and scanned for malware on shared hosting.
- 1.4 Card numbers are handled by Stripe and never stored by us. Passwords are stored hashed. Server passwords we create are shown to you once and then deleted.

2. Your part

- 2.1 Use strong, unique passwords and turn on two-step sign-in for your account.
- 2.2 Keep your websites, plugins and server software up to date.
- 2.3 Tell us straight away if you think your account has been compromised.

3. Reporting a vulnerability

- 3.1 Email hello@pricehq.tech with "**Security**" in the subject. Include what you found, where, how to reproduce it and the impact you think it has.

- 3.2 We'll acknowledge your report within 2 business days, keep you updated, and tell you when it's fixed.
- 3.3 In scope: pricehq.tech, my.pricehq.tech, mail.pricehq.tech, and our hosting and VPS platforms.
- 3.4 Out of scope: customers' own websites and servers (report those to the customer or through our Abuse Reporting process), social engineering of our staff, physical attacks, denial-of-service testing, and reports from automated scanners without a demonstrated impact.

4. Good faith and safe harbour

- 4.1 If you act in good faith, follow this policy, avoid harming people or our services, don't access, change or keep other people's data beyond what's needed to show the problem, and give us reasonable time to fix it before telling others, we won't take legal action against you or ask others to.
- 4.2 We don't currently run a paid bug bounty, but we're grateful for responsible reports and happy to credit you if you'd like.

Version history

VERSION	DATE	WHAT CHANGED
1.0	20 October 2026	First published.

Questions about this document? Email hello@pricehq.tech. PriceHQ, Australia.