Vulnerability Disclosure Policy

Last updated: March 2026

Fastcom NZ Limited ("Fastcom", "we", "us", or "our") is committed to ensuring the security and privacy of our customers, systems, and services. We value the efforts of security researchers and the broader security community in helping us identify and address potential vulnerabilities. This Vulnerability Disclosure Policy provides guidelines for security researchers to responsibly report security vulnerabilities they may discover in our publicly accessible systems and services.

Scope:

This policy applies to security vulnerabilities in:

- Our public-facing websites (e.g., *.fastcom.co.nz domains)
- Customer-facing portals and authentication systems we operate
- Public APIs and exposed services under our direct control

Out of scope (please do not test or report these under this policy):

- Third-party services or vendors (report directly to them)
- Physical attacks, social engineering, phishing, or attempts to obtain credentials
- Denial of Service (DoS/DDoS) attacks or anything that could degrade service availability
- Vulnerabilities on non-Fastcom infrastructure (e.g., customer networks, upstream providers)
- Previously known vulnerabilities or low-severity issues (e.g., missing headers without exploitability, "best practices" suggestions without security impact)
- Automated scanners that generate excessive traffic

If you are unsure whether something is in scope, please contact us before testing.

Guidelines for Security Research

We ask that you:

- Make every effort to avoid privacy violations, degradation of user experience, disruption to our services, or destruction of data.
- Only access or exfiltrate the minimum amount of data needed to prove the vulnerability (e.g., no bulk data extraction).
- Immediately stop testing and notify us if you inadvertently access customer data or sensitive information.
- Provide us with reasonable time to investigate and remediate before disclosing publicly.
- Comply with New Zealand law at all times.

Reporting a Vulnerability

If you believe you have discovered a security vulnerability within our scope, please report it to us promptly and responsibly via: email: support@fastcom.co.nz
(We aim to acknowledge reports within 2 business days and provide updates on progress.)

In your report, please include:

- A clear description of the vulnerability (including type, e.g., XSS, SQL injection, authentication bypass)
- The affected URL(s), IP(s), or endpoint(s)
- Step-by-step instructions to reproduce the issue (proof-of-concept code is welcome if safe and non-destructive)
- Any potential impact (e.g., data exposure, account takeover)
- Your contact information (or indicate if you prefer to remain anonymous)
- Any supporting evidence (screenshots, logs, etc.)

We do not currently offer monetary bounties, but we will publicly acknowledge your contribution (with your permission) once the issue is resolved, unless you prefer to remain anonymous.

What You Can Expect from Us

- We will respond to your report as quickly as possible (usually within 48 hours for initial acknowledgement).
- We will treat your report confidentially and not take legal action against good-faith reporters who follow this policy.
- We will work with you to understand and validate the issue.
- We will keep you informed of our progress toward remediation.
- We will aim to remediate valid issues in a reasonable timeframe based on severity.
- After remediation, we may invite you to confirm the fix and discuss coordinated public disclosure, should we request this we will compensate for the time and service provided.

Safe Harbor

Any activities conducted in a manner consistent with this policy will be considered authorised conduct. We will not initiate or support legal action against researchers for accidental, good-faith violations of this policy, provided they:

- Comply with the guidelines above
- Cease testing and notify us immediately upon discovering any user data
- Provide us a reasonable opportunity to remediate before public disclosure

This "safe harbour" does not apply to malicious or reckless behaviour, or to actions outside the scope of this policy.

Public Disclosure

We prefer coordinated disclosure. We ask that you:

- Allow us at least 90 days from report receipt to remediate before public disclosure (longer for critical issues requiring complex fixes or third-party coordination).
- Work with us on the timing and content of any public disclosure.

If you believe there is an immediate risk to public safety or users, please let us know so we can expedite handling.

Questions or Suggestions

If you have questions about this policy, suggestions for improvement, or need clarification on scope, please contact support@fastcom.co.nz.

We appreciate your help in keeping our services secure — thank you for acting responsibly.