

Flatpay

Responsible Disclosure Policy

March 2026

Introduction

This policy establishes a framework for security researchers to collaborate with Flatpay in identifying and addressing security vulnerabilities across our products and services. At Flatpay, we place the highest priority on security and on maintaining the trust of our customers. Responsible disclosure of security vulnerabilities plays a critical role in safeguarding the privacy and security of our users.

We are dedicated to investigating and resolving all verified security issues affecting our platforms and services in a timely manner.

We encourage you to review this document in its entirety before submitting any vulnerability reports, so that you fully understand the policy and can act in accordance with it.

This policy outlines **which systems and research types** fall within scope, **how to submit** vulnerability reports to us, and **what you can expect** from Flatpay once a report has been received.

Authorization

If you make a good faith effort to comply with this policy during your security research, we will consider your research to be authorized. We will work with you to understand and resolve the issue promptly, and Flatpay will not recommend or pursue legal action related to your research. Should legal action be initiated by a third party against you for activities conducted in accordance with this policy, we will make this authorization known.

Guidelines

Under this policy, security researchers must adhere to the following principles:

- Notify Flatpay as soon as practicable after discovering a real or potential security issue.
- Make every reasonable effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction or manipulation of data.
- Only use exploits to the extent necessary to confirm the presence of a vulnerability. Do not use an exploit to compromise or exfiltrate data, establish persistent access, or pivot to other systems.

- Do not access excessive amounts of data. For instance, retrieving 2 or 3 records is sufficient to demonstrate most vulnerabilities such as enumeration or insecure direct object reference issues.
- Do not violate the privacy of Flatpay users, employees, contractors, or customers. This includes not sharing, redistributing, or failing to properly secure any data obtained from our systems or services.
- Do not communicate any vulnerabilities or related details through methods not described in this policy, or with anyone other than your designated Flatpay security contact.
- Do not modify any data in our systems or services that does not belong to you.
- Do not disrupt our services or systems in any way.
- Provide Flatpay a reasonable amount of time to resolve the issue.
- Keep all vulnerabilities confidential until Flatpay confirms they have been fixed. The only exception is if the vulnerability also affects a third-party product (such as an open-source library) - in that case, you may notify that third party, but you must not include any details specific to Flatpay's systems. Do not submit a high volume of low-quality reports.

Once you have confirmed that a vulnerability exists or encounter any sensitive data (including personally identifiable information, financial information, or proprietary data), **you must stop your test immediately, notify us, and not disclose this data to anyone else.**

We request that any and all data retrieved during research is securely deleted as soon as it is no longer required and no later than 1 month after the vulnerability is resolved, whichever comes first.

If you are uncertain at any stage whether the actions you intend to take are acceptable, please contact our security team for guidance (do not include sensitive information in the initial communication): security@flatpay.com.

In Scope

This disclosure policy covers vulnerabilities in Flatpay products and services under the following conditions:

- Only domains and subdomains that publish a security.txt file (e.g. <https://flatpay.com/.well-known/security.txt>) are considered in scope.

Any service not expressly listed above, including any connected or third-party services, is excluded from scope and is not authorized for testing. If you are unsure whether a system falls within scope, please contact us at security@flatpay.com before beginning your research.

Out of Scope

Any services hosted by third-party providers are excluded from scope and should be reported directly to the relevant vendor in accordance with their own disclosure policy.

To protect the safety of our users, staff, the broader Internet community, and you as a security researcher, the following test types and findings are excluded from scope:

- Findings from physical testing such as office access (e.g. open doors, tailgating).

- Findings derived primarily from social engineering (e.g. phishing, vishing) or any other non-technical vulnerability testing.
- Findings from applications or systems not listed in the In Scope section above.
- UI/UX bugs and spelling mistakes.
- Network-level Denial of Service (DoS/DDoS) tests or other tests that impair access to or damage a system or data.
- TLS configuration weaknesses (e.g. weak cipher suite support, TLS 1.0 support, etc.).
- Volumetric vulnerabilities (i.e. simply overwhelming our service with a high volume of requests).
- Reports of non-exploitable vulnerabilities or reports indicating that our services do not fully align with best practice, such as missing security headers (CSP, X-Frame-Options, X-Content-Type-Options, etc.) or suboptimal email-related configuration (SPF, DMARC, etc.).

Reporting a Vulnerability

If you have identified what you believe to be an in-scope security vulnerability, please submit your report by emailing security@flatpay.com. Reports may be submitted anonymously. If you share contact information, we will acknowledge receipt of your report within 3 business days.

Your report should include:

- The website, page, or service where the vulnerability was discovered.
- A brief description of the vulnerability class (e.g. “XSS vulnerability”, “SQL injection”). Please avoid including full reproduction details at this stage — these will be requested in subsequent correspondence.
- A description of the potential impact of exploitation.

If we require additional information such as detailed reproduction steps or a proof of concept, we will provide you with a PGP key so that this sensitive information can be shared securely via encrypted communication.

In line with industry convention, we ask that reporters provide a benign (non-destructive) proof of exploitation wherever possible. This helps ensure that reports can be triaged quickly and accurately while also reducing the risk of duplicate reports or malicious exploitation for certain vulnerability classes (e.g. subdomain takeovers). Please do not include your proof of exploit in the initial plaintext email if the vulnerability remains exploitable.

What You Can Expect from Us

When you choose to share your contact information with us, we commit to coordinating with you as openly and as promptly as possible:

- Within 3 business days, we will acknowledge that your report has been received.
- Our security team will triage the reported vulnerability and respond to confirm whether further information is required and whether the report qualifies under the scope described above, or is a duplicate.

- To the best of our ability, we will confirm the existence of the vulnerability and be as transparent as possible about the steps we are taking during the remediation process, including any issues or challenges that may delay resolution.
- Priority for fixes and mitigations will be assigned based on the severity of impact and complexity of exploitation. Vulnerability reports may take some time to triage and remediate; you are welcome to enquire on the status of the process at any time.
- We will notify you when the reported vulnerability has been resolved (or when remediation work is scheduled) and will ask you to confirm that the solution adequately addresses the vulnerability.
- We will maintain an open dialogue to discuss issues throughout the process.

Bug Bounties

Flatpay does not currently offer a paid bug bounty program. We do, however, value the time and effort that security researchers invest in helping us improve our security. As a token of our gratitude, reporters of qualifying vulnerabilities will be offered a Flatpay reward.

Questions

Questions regarding this policy may be directed to security@flatpay.com. We also welcome your suggestions for improving this policy.