FounderFlow, Inc.

Vulnerability Disclosure Policy

Document Owner	Shivam Vora, Engineering Lead
Approved By	Founder & CEO, FounderFlow, Inc.
Version	1.0
Effective Date	July 22, 2026
Next Review Date	July 22, 2027
Classification	Public

This Vulnerability Disclosure Policy is a public document. FounderFlow, Inc. publishes it so that security researchers know how to report vulnerabilities to us safely and what to expect in return. A machine-readable pointer to this policy is published at **https://founderflowhq.ai/.well-known/security.txt**.

---

1. Introduction

FounderFlow, Inc. (“FounderFlow”, “we”, “us”) is committed to protecting the security of the customer data we process. FounderFlow operates an AI-powered inbox intelligence product that handles sensitive email content, calendar data, contacts, and tasks from our users’ Google Workspace accounts. We value the work of independent security researchers and believe that responsible, coordinated disclosure of vulnerabilities makes our product safer for everyone. This policy explains which systems are in scope, how to conduct testing safely, how to report what you find, and how we will respond.

2. Scope

This policy applies to the following FounderFlow-owned, internet-facing systems:

- The marketing website and web application at **founderflowhq.ai** and **www.founderflowhq.ai**
- The authenticated dashboard application (the FounderFlow front end)
- The FounderFlow backend API at **backend.founderflowhq.ai**

Out of scope. The following are explicitly out of scope and must not be tested under this policy:

- Third-party services FounderFlow integrates with or relies on — including Google (Gmail, Calendar, Cloud Platform), Stripe, HubSpot, OpenRouter, OpenAI, Anthropic, Sentry, SendGrid, Slack, Calendly, and Firebase. Vulnerabilities in these platforms should be reported to the respective vendor under their own disclosure policy.
- Any FounderFlow account, environment, or data that does not belong to you. Do not access, modify, or delete another user’s data. Use only test accounts you control.
- Findings that require physical access, social engineering, or compromise of employee devices or credentials.

If you are unsure whether a system or endpoint is in scope, email us at **hello@founderflowhq.ai** before you begin.

3. Safe Harbor / Authorization

Security research and vulnerability disclosure activities conducted in good faith and in accordance with this policy are authorized. FounderFlow will not initiate or recommend legal action against researchers for accidental, good-faith violations of this policy, and will consider such research to be authorized conduct under applicable anti-hacking laws. If legal action is initiated by a third party against a researcher who complied with this policy, we will make our authorization known. This safe harbor does not apply to activity that intentionally harms FounderFlow, its users, or third parties, or that violates the guidelines in Sections 4 and 5.

4. Researcher Guidelines

We ask that you:

- Notify us as soon as possible after you discover a real or potential security issue.
- Make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction or manipulation of data.
- Use exploits only to the extent necessary to confirm a vulnerability. Do not use an exploit to exfiltrate data, establish persistence, or pivot to other systems.
- Stop testing and notify us immediately if you encounter any sensitive data — including personal data, email content, credentials, or payment information — and keep that data strictly confidential.
- Give us a reasonable amount of time to resolve the issue before disclosing it publicly (see Section 8).
- Not submit a high volume of low-quality or automated-scanner reports without validation.

5. Prohibited Testing

The following activities are not authorized and are excluded from safe harbor:

- Network denial-of-service (DoS/DDoS) or resource-exhaustion testing, and any volumetric attack.
- Automated scanning that degrades or disrupts the service, or that ignores rate limits. Please throttle your testing.
- Social engineering (phishing, vishing, pretexting) of FounderFlow staff, users, or contractors.
- Physical attacks against FounderFlow property or personnel.
- Accessing, altering, or destroying data that does not belong to a test account you control.

6. How to Report a Vulnerability

Report all security issues by email to **hello@founderflowhq.ai**. Our published contact is also available at **https://founderflowhq.ai/.well-known/security.txt**. Reports may be submitted anonymously. Please send your report in English where possible, and encrypt sensitive details if you are able to.

7. Information to Include

To help us triage and reproduce the issue quickly, please include:

- A clear description of the vulnerability and its type.
- The affected URL, endpoint, or component (place of discovery).
- The potential impact if the issue were exploited.
- Step-by-step instructions to reproduce, including any scripts, requests, or screenshots.

8. Our Commitment and Coordinated Disclosure

When you report a vulnerability in accordance with this policy, we commit to:

- Acknowledge receipt of your report within **three (3) business days**.
- Triage and validate the report, and assign it a severity in line with our Incident Response Plan.
- Keep you reasonably informed of our progress toward a fix.
- Remediate confirmed vulnerabilities on a risk-prioritized basis — Critical and High severity issues are addressed as a priority in line with our Information Security Policy.
- Notify you when the issue is resolved, and credit you for the discovery if you wish.

We operate a **coordinated disclosure** model. We ask that you give us up to **90 days** from the date we acknowledge your report before disclosing it publicly, and that you coordinate the timing of any public disclosure with us. We are happy to discuss timelines for complex issues.

9. Recognition

FounderFlow does not currently operate a paid bug-bounty program. We are grateful for responsible disclosure and will, with your permission, publicly acknowledge researchers who help us improve the security of our product.

10. Relationship to Other Policies

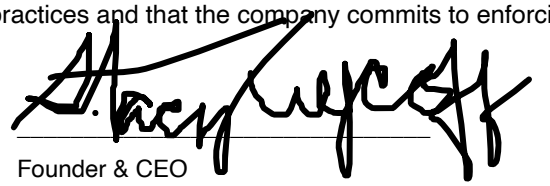
This policy works alongside the FounderFlow Information Security Policy and the FounderFlow Incident Response Plan. Confirmed vulnerabilities reported under this policy are handled as incidents under the Incident Response Plan, including containment, remediation, evidence preservation, and — where user data is affected — the notification obligations set out there.

11. Policy Review

This policy is reviewed and re-approved at least once every twelve months, or sooner following a material change to FounderFlow's systems, scope, or applicable law. The Engineering Lead is responsible for initiating the review and keeping the security.txt pointer current.

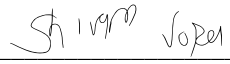
Approval and Acknowledgement

By signing below, the approving officer confirms that this policy accurately reflects FounderFlow's current practices and that the company commits to enforcing it.



Founder & CEO

Date: July 31, 2026



Engineering Lead

Date: July 31, 2026