Responsible Disclosure Policy

Last updated: 2026-03-03

Contact: security@higgsfield.ai

---

1. Introduction

Higgsfield Inc. ("we", "us", "our") takes the security of our systems and the data entrusted to us seriously. We recognize that, despite our best efforts, vulnerabilities may exist in our products and services. We value the work of security researchers and welcome responsible disclosure of any vulnerabilities discovered.

This policy sets out the terms under which security researchers may conduct vulnerability research against our systems and report findings to us. It does not grant blanket permission to conduct testing; it establishes the conditions under which we will engage with researchers in good faith and refrain from taking legal action.

---

2. Scope

In Scope

The following assets are within scope for vulnerability research:

- Web applications hosted at `https://higgsfield.ai`
- Authentication and authorization infrastructure

Out of Scope

The following are explicitly excluded:

- Third-party services and infrastructure we do not own or control
- Social engineering of Higgsfield Inc. employees, contractors, or customers
- Physical security testing of our offices or data centers
- Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks
- Spam, phishing campaigns, or any form of fraud
- Any systems or assets not listed as in scope above

If you are uncertain whether a target falls within scope, contact us at security@higgsfield.ai before proceeding.

---

3. Researcher Expectations

To qualify for our safe harbor (see Section 5), your research must conform to the following conditions.

You must:

- Conduct testing only on systems and accounts you own or have explicit written permission to test.
- Report vulnerabilities to us promptly after discovery, before any public disclosure.
- Provide sufficient information for us to reproduce and verify the finding (see Section 4).
- Allow us a reasonable period to remediate before any public disclosure (see Section 6).

You must not:

- Access, download, modify, or delete data belonging to any user or third party.
- Execute or attempt to execute code on our systems beyond what is strictly necessary to demonstrate the vulnerability.
- Pivot to or attempt to access systems outside the defined scope.
- Disrupt the availability or integrity of any production system or service.
- Conduct any testing that could degrade the experience of legitimate users.
- Disclose the vulnerability to any third party (including bug bounty aggregators) without our written consent prior to remediation.

---

4. Reporting a Vulnerability

Please submit your report to: security@higgsfield.ai

Where possible, encrypt your report using our PGP key, available at:

`https://higgsfield.ai/.well-known/pgp-key.txt`

Fingerprint: `CD77 164C 67EE 0FBB 73AD  DC69 48CC E83B 1131 44A1`

A useful report includes the following:

- A clear description of the vulnerability and its potential impact.

- The affected asset (URL, application name, API endpoint).
- Step-by-step reproduction instructions, including any tools, scripts, or payloads used.
- Screenshots, videos or proof-of-concept code that demonstrates the issue.
- Your assessment of severity.
- Any suggested remediation you consider appropriate.

The more detail you provide, the faster we can triage and remediate.

---

5. Our Commitments

When you report in accordance with this policy, we commit to the following:

- **Acknowledgement.** We will acknowledge receipt of your report within **3 business days**.
- **Triage.** We will provide an initial triage assessment within **10 business days**.
- **Communication.** We will keep you informed of our progress at regular intervals throughout the remediation process.
- **Remediation.** We will work diligently to remediate confirmed vulnerabilities within a timeframe proportionate to severity. We will notify you when remediation is complete.
- **Recognition.** With your permission, we will recognize your contribution in our Security Hall of Fame.
- **No legal action.** Provided you comply with this policy and act in good faith, we will not pursue civil or criminal action against you, nor will we refer your conduct to law enforcement agencies.

We do not currently operate a paid bug bounty program. This policy does not create an obligation for financial reward.

---

6. Coordinated Disclosure

We follow a coordinated disclosure model. We ask that you:

1. Report the vulnerability to us privately before any public disclosure.
2. Allow us a minimum of **90 calendar days** from the date of acknowledgement to remediate before you publish or discuss the findings publicly.
3. If circumstances require earlier disclosure (e.g. active exploitation in the wild), contact us immediately to discuss an accelerated timeline.

We will endeavor to remediate critical and high-severity findings well within the 90-day window and will proactively contact you to agree a disclosure date once a fix is in place.

If we are unable to remediate within 90 days, we will communicate this to you with an explanation and proposed revised timeline. We will not seek to suppress or delay disclosure indefinitely.

---

7. Out-of-Scope Submissions

The following vulnerability classes are generally considered out of scope and will not typically result in remediation action, recognition, or safe harbor:

- Missing security headers with no demonstrated exploitability (e.g. `X-Frame-Options` on pages without sensitive content).
- SPF, DKIM, or DMARC configuration issues without demonstrated mail spoofing impact.
- SSL/TLS configuration reports without demonstrated exploitability.
- Rate limiting issues that require unrealistic request volumes.
- Self-XSS or vulnerabilities that require victim interaction equivalent to shooting oneself in the foot.
- Username or email enumeration without demonstrated material security impact.
- Lack of informational files similar to security.txt, robots.txt.
- Reports generated entirely by automated scanners with no manual verification.

We may still review and act on out-of-scope submissions at our discretion, but we cannot commit to the same timelines or safe harbour protections.

---

8. Legal

This policy is not a contract and does not create any legally binding obligations on either party beyond those that apply by law. It represents our good-faith commitment to researchers who engage with us responsibly.

Researchers are responsible for ensuring their activities comply with applicable laws in their jurisdiction. This policy does not authorize any activity that would be unlawful regardless of our consent, including but not limited to accessing accounts or data belonging to third parties.

Higgsfield Inc. reserves the right to amend this policy at any time.

---

9. Acknowledgements

We are grateful to the researchers listed on our Security Hall of Fame for their contributions to the security of our systems.