

Vulnerability Disclosure Policy

Version: 1.0

Date: 2026-06-15

Author: Andreas Åström

1. Purpose and Scope

Paraglide is committed to the security of our customers and their data. This policy provides guidelines for security researchers to conduct vulnerability discovery activities and to submit discovered vulnerabilities to us. It also defines our internal procedures for triaging and remediating these reports.

This policy applies to all systems and services owned or operated by Paraglide, including the Paraglide AI Platform and the paraglide.com domain.

2. Safe Harbor

Paraglide will not take legal action against researchers who discover and report vulnerabilities in good faith and comply with the guidelines in this policy. We consider any research conducted under this policy to be:

- Authorized in accordance with the Computer Fraud and Abuse Act (CFAA) (and/or similar local laws).
- Exempt from the Digital Millennium Copyright Act (DMCA), and we will not bring a claim against you for circumvention of technological measures.
- Lawful, helpful to the overall security of the Internet, and conducted in good faith.

3. Reporting Guidelines

If you believe you have found a security vulnerability, please submit it via the contact method specified in our security.txt file at <https://app.paraglide.ai/.well-known/security.txt>.

Reports should include:

- A description of the location and nature of the vulnerability.
- Detailed steps to reproduce the vulnerability (Proof of Concept).
- Any screenshots or videos that may assist in triage.

4. Out-of-Scope Activities

To protect our users and employees, the following activities are strictly prohibited and considered out-of-scope:

- **Social Engineering/Phishing:** Any attempt to deceive or phish Paraglide employees or contractors.
- **Denial of Service (DoS/DDoS):** Any activity that degrades the performance or availability of our services.
- **Third-Party Systems:** Vulnerabilities in third-party software or integrations (e.g., Gmail, Outlook, Xero) should be reported directly to those vendors.
- **Physical Security:** Any attempt to gain physical access to Paraglide offices or data centers.
- **Data Privacy:** Accessing, downloading, or modifying data that does not belong to you. If you accidentally encounter private data, stop immediately and report it.

5. Triage and Remediation Procedures

Upon receipt of a report, Paraglide personnel will follow these internal procedures:

5.1 Intake & Acknowledgment

The security team will acknowledge receipt of the report within 3 business days.

5.2 Triage and Risk Assessment

Vulnerabilities will be assessed based on Likelihood and Impact according to the **Paraglide Risk Management Policy**.

- **P0 (Critical)**: Active exploitation or high risk to PII.
- **P1 (High)**: Direct risk of exploitation or malware.
- **P2 (Medium)**: Significant risk requiring complex prerequisites.
- **P3 (Low)**: Theoretical or low-impact issues.

5.3 Remediation SLAs

Verified vulnerabilities must be remediated according to the timelines defined in the **Operations Security Policy**:

- **Critical/High**: 30 Days
- **Medium**: 60 Days
- **Low**: 90 Days

6. Exceptions and Violations

Failure to follow the guidelines in this policy may result in the loss of Safe Harbor protections and, in the case of employees or contractors, disciplinary action up to and including termination.

7. Version History

Version	Date	Description	Author	Approved By
1.0	2026-06-15	Initial Version	Andreas Åström	Christoffer Flystam