



Vulnerability Disclosure Policy

At **Vaneigens**, the security of our systems and the protection of our customers' data are our top priorities. Despite our efforts to maintain a secure environment, vulnerabilities may still exist. We appreciate the help of the security research community in identifying and reporting these issues.

If you have discovered a security vulnerability in our own software or our infrastructure, we want to hear from you.

1. Reporting a Vulnerability

If you believe you have found a security vulnerability, please submit your report to us at **security@vaneigens.com**. Please include the following information in your report:

- A detailed description of the vulnerability.
- The specific URL, application, or system affected.
- Steps to reproduce the issue (e.g., scripts, screenshots, or screen recordings).
- The potential impact of the vulnerability.

2. Our Scope

This policy applies to:

- Software products developed and owned by **Vaneigens**.
- Our corporate website and public-facing infrastructure.

Third-Party Software: As a service provider, we also implement software from third-party vendors. If you find a vulnerability in a third-party product that we use or implement for clients:

- We will coordinate with the vendor to ensure the issue is addressed.
- However, the final remediation and "Safe Harbor" protection are subject to that vendor's own disclosure policies.

3. Guidelines & Rules of Engagement

To protect our users and systems, we ask you to follow these rules:

- **Do no harm:** Avoid any actions that could disrupt our services (e.g., DoS/DDoS attacks) or compromise user data.
- **Privacy first:** Do not access, modify, or delete data that does not belong to you.
- **No Social Engineering:** Do not use phishing, spam, or physical security attacks against our employees or offices.
- **Confidentiality:** Do not disclose the vulnerability to the public or third parties until we have had a reasonable amount of time to fix it.



4. Our Commitment

If you follow the guidelines above, we commit to the following:

- **Acknowledgment:** We will acknowledge receipt of your report within five business days.
- **Safe Harbor:** We will not take legal action against you or ask law enforcement to investigate, provided you act in good faith and comply with this policy.
- **Updates:** We will keep you informed of our progress as we work to remediate the vulnerability.

Latest update: 01-01-2026