AKASCAN – Responsible Disclosure Policy

Version 1.0 — Last updated: November 14, 2025

AKASEC B.V. is committed to ensuring the security of our systems and the privacy of our customers. This Responsible Disclosure Policy explains how security researchers can report vulnerabilities to us safely and responsibly.

---

1. Introduction

If you discover a security vulnerability in AKASCAN or related infrastructure, we ask that you report it to us responsibly. We do **not** pursue legal action against good-faith researchers who follow this policy.

---

2. Scope

This policy applies to:

- The AKASCAN platform
- API endpoints
- *.akascan.com infrastructure
- Authentication and account management
- Report storage
- Domain verification flows
- Any backend systems processing customer scans

Out of scope:

- Domains or systems not owned by AKASEC
- Social engineering of employees or customers
- Physical security attacks

- DDoS or brute-force stress testing
- Automated scanning on third-party infrastructure

---

3. How to Report a Vulnerability

Please include:

1. A description of the vulnerability
2. Steps to reproduce
3. Impact assessment
4. Any relevant technical details or proof-of-concept
5. Contact information for follow-up

Send reports to: **security@akasec.com**

---

4. What We Ask From You

- Act in **good faith**
- Do not exploit the vulnerability
- Do not access more data than necessary
- Do not modify or delete data
- Do not disrupt the service
- Give us a reasonable amount of time to fix the issue before public disclosure
- Keep the vulnerability confidential until we confirm it is resolved

---

5. What You Can Expect From Us

- We confirm receipt within **5 business days**

- We aim to provide a fix or mitigation within **30 days**
- We will keep you updated during the process
- We will credit you publicly (if desired)
- We will not take legal action if the report is made under this policy and in good faith

---

6. Prohibited Actions

The following are not permitted:

- Launching DDoS attacks
- Running automated scanners at high frequency
- Attempting to access other customers' data
- Social engineering
- Physical intrusion
- Spamming or phishing campaigns
- Ransom / extortion attempts

---

7. Recognition

We are grateful for contributions that help us improve our platform.
With your permission, we may list your name in a future "Security Hall of Fame".

(No bug bounties at this time, but we may introduce them later.)

---

8. Legal Safe Harbor

If you follow this policy in good faith:

- You will not be prosecuted
- We will not take civil action
- We consider your actions authorized under Dutch law for the purpose of responsible disclosure

If law enforcement becomes involved, we will clarify that your actions were performed responsibly.

---

9. Updates to This Policy

We may revise the policy over time.

The latest version will always be available on our website.

---

10. Contact

For vulnerability reports:

security@akasec.com

For general questions:

hello@akasec.com
