Vulnerability Disclosure Policy

AK Touch Secure

At **AK Touch Secure™**, we are committed to maintaining the security and privacy of our users, systems and data. Security researchers and members of the community play an essential role in helping us meet this goal. We welcome and encourage responsible disclosure of vulnerabilities that may affect our services or infrastructure.

This Vulnerability Disclosure Policy outlines how to report vulnerabilities, what to expect from us, and the guidelines for responsible security research.

Scope

This policy applies to:

- All public-facing systems and services operated by **AK Touch Secure™**.
- Mobile applications, APIs and web applications under the aktouchsecure.com domain or subdomains.
- Backend infrastructure directly supporting our products or user data.

If you are unsure whether a system is in scope, please contact us before starting your research.

Reporting a Vulnerability

If you believe you have discovered a vulnerability in one of our systems, please report it by emailing: **sales@kenricks.co.uk**.

Your report should include:

- A detailed description of the vulnerability.
- Steps to reproduce the issue.
- Any relevant screenshots, logs, or proof-of-concept code.
- The potential impact and any mitigation you may suggest.

We encourage PGP encryption for sensitive disclosures.

KENRICK

Call: **0121 500 3266**
Email: **sales@kenricks.co.uk**

Union Street • Kenrick Way • West Bromwich • B70 6DB

www.kenricks.co.uk

Vulnerability Disclosure Policy

Our Commitment

When you report a vulnerability under this policy, AK Touch Secure™ commits to:

- **Acknowledgment** – We will acknowledge receipt of your report within 5 business days.
- **Investigation** – We will investigate and validate the reported issue promptly.
- **Remediation** – If a valid vulnerability is confirmed, we will work to address it as quickly as possible.
- **Transparency** – We will keep you informed of our progress throughout the remediation process.
- **Credit** – With your permission, we will credit your responsible disclosure in our security acknowledgements page.

Responsible Research Guidelines

To protect our users and services, we require that you:

- Do not exploit the vulnerability beyond what is necessary to demonstrate the issue.
- Do not access, modify, or delete any data that does not belong to you.
- Do not engage in any activity that could cause harm, degrade service, or violate applicable laws.
- Avoid automated scanning or denial of service (DoS) attacks.

We do not pursue legal action against researchers who act in good faith and abide by this policy.

Out of Scope Vulnerabilities

Some findings are generally considered out of scope unless evidence suggests a severe impact.

These may include:

- Rate limiting or brute force issues without practical exploit.
- Clickjacking on non-sensitive pages.
- Use of known or public software versions.
- Lack of DNSSEC.
- Missing security headers (e.g., CSP) without demonstrable exploitability.

Safe Harbor

AK Touch Secure™ pledges not to initiate legal action against researchers who:

- Follow this policy in good faith.
- Report vulnerabilities without demanding compensation.
- Do not exploit or abuse the vulnerability.

We view responsible disclosure as an important part of improving our security posture.

Questions?

If you have any questions about this policy, please contact us at: sales@kenricks.co.uk. Thank you for helping keep AK Touch Secure™ safe and secure.

KENRICK

Call: **0121 500 3266**
Email: **sales@kenricks.co.uk**

Union Street • Kenrick Way • West Bromwich • B70 6DB

www.kenricks.co.uk