AKASCAN – Terms & Conditions

Version 1.0 — Last updated: November 14, 2025

These Terms & Conditions ("Terms") govern the use of the AKASCAN platform ("Platform"), operated by **AKASEC B.V.** ("we", "us", "our"). By creating an account or using the Platform, the customer ("Customer", "you", "your") agrees to these Terms.

---

1. Definitions

- **Platform:** The AKASCAN web application and related services.
- **Asset / Domain:** Any domain submitted by the Customer for verification and scanning.
- **Verification Record:** A TXT record provided via the Platform to prove ownership of a domain.
- **Report:** The monthly vulnerability assessment generated by us for each verified domain.
- **Service:** Continuous external vulnerability scanning and reporting performed by AKASCAN.

---

2. Eligibility & Account Registration

2.1. To use the Platform, the Customer must create an account and provide accurate information.
2.2. Customers are responsible for keeping login credentials confidential.
2.3. AKASCAN may suspend accounts in case of suspected abuse, fraud, or security risk.

---

3. Domain Verification

3.1. The Customer adds one or more domains ("Assets") to the Platform.
3.2. The Platform generates a **unique TXT record** that must be added to the Customer's DNS.
3.3. Verification proves domain control and authorizes AKASCAN to scan that domain.

3.4. By verifying a domain, the Customer confirms that:

- They own or have explicit permission to scan the domain
- Scanning this domain is legal in their jurisdiction
- AKASCAN is authorized to perform automated assessments

3.5. AKASCAN may refuse or remove unverified or suspicious domains.

---

4. Scope of the Service

4.1. Once a domain is successfully verified:

- We receive an internal notification
- The domain is added to our backend vulnerability-scanning system
- Continuous security scans are executed automatically

4.2. The Service includes:

- Automated external vulnerability scanning of the verified domain
- Monthly reports containing findings and recommended remediation steps
- Secure hosting of generated reports in the Customer’s portal

4.3. The Service **does not** include:

- Penetration testing
- Social engineering
- Incident response
- Internal network assessments
- Remediation of vulnerabilities

(Separate agreements may be made for additional services.)

---

5. Monthly Reports

5.1. Reports are generated once per month per verified asset.

5.2. Reports are uploaded to the Customer portal for download.

5.3. Reports contain confidential information and must be handled securely by the Customer.

---

6. Customer Responsibilities

The Customer agrees to:

- Only submit domains they own or control
- Properly configure DNS verification records
- Not misuse the Platform to scan unauthorized systems
- Act upon vulnerabilities responsibly
- Ensure employees or contractors accessing reports follow secure handling practices

---

7. Prohibited Use

The Platform may not be used to:

- Scan systems you do not own
- Perform offensive cyber activities
- Attempt to breach, overload, or manipulate the Platform
- Reverse engineer or copy the Platform's functionality

Violation may result in immediate account termination and potential legal action.

---

8. Availability & Maintenance

8.1. AKASCAN strives for high availability but does not guarantee uninterrupted uptime.
8.2. Planned maintenance may occur and will be announced when possible.
8.3. AKASCAN is not liable for:

- Downtime
- Delay in report generation
- Data loss due to Customer misconfiguration

---

9. Security & Data Protection

9.1. We store Customer data (including domains and reports) securely.
9.2. Sensitive findings are accessible only to authenticated Customer accounts.
9.3. Payment details (if applicable) are processed by third-party providers and never stored by us.
9.4. We comply with GDPR for EU Customers.

---

10. Fees & Billing

10.1. Pricing is available on the AKASCAN website or via quotation.
10.2. Services are billed monthly or annually.
10.3. Non-payment may result in suspension of scanning and report availability.

---

11. Limitation of Liability

11.1. AKASCAN provides scanning and reporting on a **best-effort basis**.
11.2. We do **not** guarantee detection of all vulnerabilities.

11.3. AKASCAN is not liable for:

- Security incidents occurring before or after the scan
- Losses caused by Customer inaction
- Damages resulting from misconfigured systems or failure to apply remediations

11.4. Maximum liability is limited to the fees paid in the previous 12 months.

---

12. Confidentiality

Reports and findings may not be shared publicly without written permission from AKASEC.
We treat all Customer data as confidential.

---

13. Termination

13.1. Customers may terminate the Service at any time via the Platform.
13.2. AKASCAN may terminate access for:

- Abuse
- Non-payment
- Security threats
- Legal concerns

13.3. After termination:

- Scans stop
- Reports remain available for 30 days
- Data may be permanently deleted afterward

---

14. Changes to the Terms

AKASCAN may update these Terms. Continued use of the Platform constitutes acceptance of the updated Terms.

---

15. Governing Law

These Terms are governed by **Dutch law**.
Disputes are handled exclusively by the courts of **The Hague, The Netherlands**.

---

16. Contact

AKASEC B.V.
Wilhelmina van Pruisenweg 104
2595 AN, The Hague
The Netherlands
Email: hello@akasec.com
