

Security4Web3

Terms of Service

Effective Date: 8 June 2026 | Institutional Grade Blockchain Security Consultancy

By engaging Security4Web3 ('the Company', 'we', 'our', 'us') for any service, you ('the Client', 'you') agree to the following Terms of Service ('Agreement'). This Agreement governs all engagements, including but not limited to security reviews, penetration testing, operational security reviews, compliance advisory, formal verification, and related consultancy services ('the Services'). If you do not agree to these terms, do not engage our Services.

1. Scope of Services

Security4Web3 provides institutional-grade security consultancy for blockchain projects, digital asset businesses, and organisations operating in or transitioning to on-chain environments. Our Services include, but are not limited to:

- **Smart Contract Security Reviews:** Independent review of smart contract code to identify vulnerabilities, logic errors, and deviations from specification across EVM, Solana, Cosmos, and other ecosystems.
- **Operational Security Reviews:** Comprehensive assessment of people, processes, and technology controls — including insider threat analysis, access management (IAM/PAM), RBAC design, secure data handling, hardware encryption policy, hiring security vetting, and onboarding/offboarding procedures.
- **Penetration Testing:** Adversarial testing of decentralised applications, Web3 APIs, blockchain node infrastructure, and supporting systems. Includes social engineering assessments and phishing simulations.
- **Human Factors & Insider Threat Reviews:** Assessment of human-layer risk, including role-based access design, personnel vetting, security culture, and insider threat detection.
- **Key Ceremony & Multisig Governance:** Design and facilitation of key generation ceremonies, multisignature wallet governance structures, and private key storage solutions including HSM and MPC architectures.
- **Regulatory Compliance Advisory:** Structured security reviews evidencing alignment with DORA, MiCA, VARA, DASP, and equivalent regulatory frameworks for digital asset businesses.
- **Formal Verification:** Mathematical proof-based verification of smart contract correctness for high-assurance environments.
- **Incident Response Planning:** Development of incident response playbooks, tabletop exercises, and post-incident review services.

All engagements are scoped individually in a written Statement of Work ('SOW') agreed prior to commencement. Services are delivered against that defined scope only.

2. Service Limitations

Our Services are designed to provide thorough, professional security assessments informed by current knowledge, tooling, and industry best practice at the time of engagement. However:

- No security review can guarantee that a system is entirely free from vulnerabilities. New attack vectors, dependency changes, and unforeseen conditions may arise after our engagement concludes.

- Our findings represent a point-in-time assessment bounded by the agreed scope. Material changes to code, infrastructure, or configuration after delivery of our report are outside the scope of the engagement.
- Completion of a security review does not constitute an endorsement of the project, its token, its governance, or its commercial viability.
- Operational security reviews assess the controls present at the time of engagement. The effectiveness of those controls depends on consistent implementation by the Client.

3. Liability and Indemnification

The Client acknowledges that it is solely responsible for the operation, security posture, legal standing, and regulatory compliance of its project. Security4Web3 shall not be held liable for any losses, damages, regulatory penalties, or reputational harm arising from:

- Security incidents, exploits, or breaches occurring after delivery of our report.
- The Client's failure to remediate findings identified in our report.
- Modifications made to code, infrastructure, or processes after our engagement concludes.
- Third-party dependencies, integrations, or services outside the agreed review scope.
- Regulatory enforcement actions, regardless of whether a compliance review was conducted.

The Client agrees to indemnify and hold Security4Web3, its directors, employees, and contractors harmless against any claims, damages, or losses arising from the Client's use of our Services or reliance on our reports.

4. Confidentiality

Security4Web3 treats all Client information as strictly confidential. We will not disclose proprietary data, engagement details, findings, or report contents to any third party without the Client's explicit written consent, except where required by applicable law or regulatory authority.

Clients are encouraged to implement responsible disclosure practices for vulnerabilities identified during our engagement. Security4Web3 may, with Client consent, publish anonymised case studies or general methodology content.

5. Engagement Outcome and Payment Policy

By engaging Security4Web3 and confirming a Statement of Work, the Client acknowledges:

- **No Guaranteed Outcome:** Payment does not guarantee a specific result. Security review findings are determined solely by our objective professional assessment.
- **Non-Refundable Fees:** Engagement fees cover the time, expertise, and resources allocated to the review, regardless of findings. Fees are non-refundable once work has commenced.
- **Critical Findings:** Where critical vulnerabilities or operational control failures are identified, this does not constitute grounds for refund, legal action, or reputational claims against Security4Web3. Our role is to assess and report; remediation is the Client's responsibility.
- **Operational Reviews:** For operational security reviews, findings represent the state of controls at the time of assessment. Remediation plans and prioritisation remain at the Client's discretion.

6. Acceptance of Terms

By engaging our Services — whether through a signed Statement of Work, written instruction, or payment — the Client confirms they have read, understood, and accepted this Agreement in full.

7. Changes to These Terms

Security4Web3 reserves the right to amend these Terms of Service at any time. Updated terms will be published on our website and take effect immediately upon posting. Continued engagement with our Services following any update constitutes acceptance of the revised terms.