AIConsensusAudit.com Terms of Service

Effective Date: July 6, 2026These Terms of Service, together with any documents incorporated by reference, including any privacy policy, token disclaimers, payment terms, or additional platform rules, govern your access to and use of **AIConsensusAudit.com**, including any related websites, applications, APIs, reports, smart-contract scanning tools, artificial intelligence audit features, token-based payment features, and related services. These Terms are entered into between you and **[Company Legal Name]**, doing business as **AI Consensus Audit**, **AIConsensusAudit.com**, or any affiliated brand names used in connection with the platform. For purposes of these Terms, **"AI Consensus Audit," "we," "us," or "our"** refers to **[Company Legal Name]**. **"User," "you," or "your"** refers to any person or entity accessing or using the Services. By accessing or using the Services, connecting a wallet, submitting code, purchasing a scan, using $AICA, or otherwise interacting with the platform, you agree to be bound by these Terms. If you do not agree, do not use the Services.

---

1. Definitions

For purposes of these Terms: **"Services"** means the AIConsensusAudit.com website, smart-contract scanning engine, AI audit tools, reports, APIs, dashboards, payment systems, token-related functionality, and any related products or services. **"Scan"** means an automated or AI-assisted review of submitted code, smart contracts, repositories, files, or related materials. **"Report"** means any output generated by the Services, including vulnerability findings, risk scores, architecture maps, exploitability notes, recommendations, explanations, or other analysis. **"Submitted Materials"** means any code, smart contracts, repositories, files, documentation, metadata, prompts, comments, or other content you upload, paste, link, submit, or otherwise provide to the Services. **"$AICA"** means the utility token associated with AIConsensusAudit.com, which may be used for payment or access to certain platform features. **"User Content"** means any content, code, materials, data, or information submitted by you or on your behalf.

---

2. Eligibility

You may use the Services only if you are legally able to enter into a binding agreement. By using the Services, you represent and warrant that:

1. **You are at least 18 years old**, or the age of majority in your jurisdiction.
2. **You have authority** to bind any entity on whose behalf you use the Services.
3. **Your use of the Services is lawful** in your jurisdiction.

4. **You are not located in, organized in, or ordinarily resident in any sanctioned jurisdiction.**
5. **You are not subject to sanctions**, export controls, or restrictions that would prohibit your use of the Services.
6. **You will not use the Services for unlawful, harmful, abusive, or prohibited purposes.**

We may refuse, suspend, restrict, or terminate access to the Services at any time if we believe you do not meet these requirements.

---

3. Nature of the Services

AIConsensusAudit.com provides **AI-assisted smart-contract security analysis**. The Services may use independent AI models, automated code analysis, evidence-weighted scoring, exploitability checks, report generation, and related techniques to identify potential security issues in submitted code. However, you acknowledge and agree that:

1. **The Services are automated and AI-assisted.**
2. **Reports may contain errors, omissions, false positives, or false negatives.**
3. **The Services do not guarantee detection of all vulnerabilities.**
4. **The Services do not guarantee that any code is safe, secure, complete, correct, production-ready, or free from defects.**
5. **The Services are not a substitute for professional manual audits, legal review, economic review, formal verification, penetration testing, or independent security assessment.**

AI Consensus Audit is intended to assist developers, protocols, auditors, and teams by providing security-related analysis, but final responsibility for reviewing, testing, deploying, modifying, or relying on any code remains solely with you.

---

4. No Security Guarantee

You understand and agree that **no automated scan, AI model, consensus system, or security tool can guarantee the security of smart-contract code**. Even if a Report shows no critical or high-risk findings, your code may still contain vulnerabilities. Even if a finding is marked low confidence, uncertain, refuted, or informational, the underlying issue may still present real-world risk depending on context. You are solely responsible for:

- **Reviewing all Reports**
- **Testing your code**

- **Obtaining manual audits where appropriate**
- **Assessing business logic and economic assumptions**
- **Validating fixes**
- **Determining whether code is safe to deploy**
- **Managing protocol risk**
- **Protecting user funds**
- **Complying with applicable laws and regulations**

You agree that you will not rely on the Services as your sole basis for deploying, upgrading, operating, or securing any smart contract, protocol, application, token, wallet, bridge, DAO, marketplace, or other blockchain-based system.

---

5. No Professional Advice

The Services and Reports are provided for informational and technical assistance purposes only. They do not constitute:

- **Legal advice**
- **Financial advice**
- **Investment advice**
- **Tax advice**
- **Regulatory advice**
- **Accounting advice**
- **Professional security certification**
- **Formal audit attestation**
- **Insurance coverage**
- **Compliance approval**
- **Guarantee of code safety**

You should consult qualified professionals before making decisions involving legal obligations, financial risk, regulatory compliance, user funds, production deployment, or other material matters.

---

6. User Responsibility for Submitted Materials

You are solely responsible for all Submitted Materials. By submitting code, repositories, files, documents, links, or other materials to the Services, you represent and warrant that:

1. **You own the Submitted Materials or have all rights necessary to submit them.**
2. **Your submission does not violate any confidentiality obligation, license, contract, law, regulation, or third-party right.**
3. **Your submission does not contain malware, malicious code, stolen materials, trade secrets you are not authorized to disclose, or illegal content.**
4. **You have authority to request analysis of the submitted code.**
5. **Your use of the Services will not violate intellectual property, privacy, security, or contractual rights of any third party.**

We are not responsible for determining whether you have the right to submit any code or materials.

---

7. License to Analyze Submitted Materials

You retain ownership of your Submitted Materials. However, by submitting materials to the Services, you grant AI Consensus Audit a worldwide, non-exclusive, royalty-free, sublicensable, transferable license to access, process, transmit, store, analyze, transform, and use the Submitted Materials as reasonably necessary to:

- **Provide the Services**
- **Generate Reports**
- **Operate the platform**
- **Debug and improve scan functionality**
- **Maintain security and abuse prevention**
- **Provide customer support**
- **Comply with legal obligations**
- **Enforce these Terms**

We do not claim ownership of your submitted code. If you use third-party integrations, repositories, wallets, APIs, cloud services, model providers, or hosting systems in connection with the Services, your materials may also be subject to the terms and policies of those third parties.

---

8. Confidentiality and Sensitive Code

We understand that smart-contract code may be sensitive. We will use commercially reasonable efforts to protect Submitted Materials. However, you acknowledge that:

1. **No online service is perfectly secure.**

2. **Transmission and processing of code may involve third-party infrastructure or AI model providers.**
3. **You should not submit materials that you are not authorized to share.**
4. **You should not submit private keys, seed phrases, passwords, confidential credentials, unpublished exploits, or highly sensitive information unless specifically instructed and protected by a separate written agreement.**

You are solely responsible for removing secrets, credentials, private keys, environment variables, and other sensitive data before submission. We are not liable for losses resulting from your submission of sensitive or unauthorized materials.

---

9. API and Repository Access

If you connect a repository, wallet, API key, integration, or third-party account to the Services, you authorize us to access and process the connected materials as necessary to provide the Services. You are responsible for:

- **Configuring access permissions**
- **Revoking access when no longer needed**
- **Ensuring repository access is authorized**
- **Managing API keys and credentials**
- **Monitoring use of connected integrations**

We may suspend API or repository access if we detect abuse, excessive usage, security risks, unauthorized activity, or violation of these Terms.

---

10. Reports and Output

Reports are generated using automated tools, AI systems, model outputs, scoring logic, and related analysis. You acknowledge that Reports:

1. **May be incomplete or inaccurate.**
2. **May misclassify severity, exploitability, or confidence.**
3. **May omit vulnerabilities.**
4. **May include false positives.**
5. **May recommend fixes that require further review.**
6. **May depend on limited context provided by you.**

7. **May not account for all deployment, governance, oracle, economic, or runtime conditions.**

You are solely responsible for reviewing, validating, testing, and applying any recommendations. We do not guarantee that any Report will identify all vulnerabilities or prevent losses.

---

11. No Emergency Monitoring or Incident Response

Unless expressly agreed in a separate written agreement, the Services do not provide:

- **Real-time monitoring**
- **Emergency incident response**
- **Exploit recovery**
- **Key compromise response**
- **Live threat blocking**
- **Insurance**
- **On-chain intervention**
- **Asset recovery**
- **Legal enforcement support**

If you believe your protocol has been exploited or is at immediate risk, you should contact qualified security professionals immediately.

---

12. Payments

Certain Services may require payment. Full scans are priced at **$100** with standard payment methods, unless otherwise stated at checkout. Users who pay with **AICA** may access the preferred platform scan rate of **\50** per eligible full scan, unless otherwise stated at checkout. Prices, supported payment methods, promotional offers, scan limits, included features, and eligibility requirements may change at any time. All prices are displayed before purchase where required. You are responsible for all blockchain network fees, gas fees, exchange fees, slippage, taxes, wallet fees, and other costs associated with payment.

---

13. Crypto Payments

Crypto transactions are generally irreversible. By paying with cryptocurrency, stablecoins, $AICA, or any other digital asset, you acknowledge and agree that:

1. **Blockchain transactions cannot usually be reversed.**
2. **You are responsible for sending payment to the correct address.**
3. **You are responsible for using the correct network.**
4. **You are responsible for gas fees and transaction costs.**
5. **We are not responsible for failed, delayed, misdirected, underpaid, or overpaid transactions caused by user error, wallet issues, network congestion, third-party services, or blockchain failures.**
6. **Token prices or conversion rates may fluctuate.**
7. **Checkout calculations may be based on then-current platform pricing or third-party pricing data.**

We may, but are not required to, assist with payment issues.

---

14. Refund Policy

Unless otherwise required by applicable law or expressly stated in writing, **all paid scans are final and non-refundable once processing begins**. We may issue refunds, credits, or replacement scans at our sole discretion in cases such as:

- **Platform processing failure**
- **Duplicate payment**
- **Material technical error caused by us**
- **Scan not delivered due to platform fault**

We do not provide refunds because:

- You disagree with a Report.
- A Report did not find vulnerabilities.
- A Report found vulnerabilities you believe are inaccurate.
- A later manual audit reaches a different conclusion.
- You submitted the wrong code.
- You used the wrong wallet, chain, token, or payment method.
- You experienced crypto price movement.

- You no longer need the scan.
- Your code or deployment plan changed after purchase.

---

15. $AICA Token Disclaimer

$AICA is intended as a utility token for use within the AI Consensus Audit ecosystem.$AICA may be used for:

- **Scan payments**
- **Preferred scan pricing**
- **API usage**
- **Continuous re-scans**
- **Advanced platform features**
- **Security research grants**
- **Ecosystem participation**
- **Other platform-related utilities that may be added over time**

$AICA does not represent or provide:

- **Equity**
- **Ownership**
- **Voting control over company operations**
- **Revenue share**
- **Profit rights**
- **Dividends**
- **Passive income**
- **Claims on assets**
- **Debt**
- **Investment contract rights**
- **Any promise of future value**

We make no representation regarding the market price, liquidity, availability, exchange listing, transferability, tax treatment, regulatory treatment, or future utility of $AICA. You are solely responsible for determining whether acquiring, holding, using, transferring, or disposing of $AICA is lawful in your jurisdiction.

---

16. Token Availability and Restrictions

We may restrict, block, limit, or refuse $AICA-related functionality in certain jurisdictions, for certain users, or under certain circumstances. We may do so for legal, compliance, sanctions, security, technical, business, or risk-management reasons. We are not obligated to support $AICA payments in every jurisdiction, on every chain, through every wallet, or indefinitely. We may modify, suspend, or discontinue token-related features at any time, subject to applicable law.

---

17. Taxes

You are solely responsible for determining and paying any taxes, duties, levies, reporting obligations, or other governmental charges arising from your use of the Services, crypto payments, $AICA transactions, token acquisitions, token disposals, scan purchases, or related activity. We do not provide tax advice.

---

18. Prohibited Uses

You agree not to use the Services to:

1. Violate any applicable law, regulation, sanctions rule, export control, or third-party right.
2. Submit code you are not authorized to analyze.
3. Upload malware, viruses, worms, ransomware, spyware, credential stealers, or harmful content.
4. Generate, improve, or facilitate malicious exploits against systems you do not own or have authorization to test.
5. Attack, probe, overload, disrupt, scrape, reverse engineer, or abuse the Services.
6. Circumvent payment systems, access controls, rate limits, API limits, token gates, or usage restrictions.
7. Interfere with model providers, infrastructure providers, payment systems, wallets, or third-party integrations.
8. Use the Services to violate intellectual property, confidentiality, privacy, or contractual obligations.

9. Misrepresent Reports as official certification, insurance, legal approval, regulatory approval, or guaranteed security clearance.
10. Resell, white-label, copy, or commercialize the Services without written permission.
11. Use the Services for sanctioned, restricted, fraudulent, deceptive, or illegal activity.
12. Upload private keys, seed phrases, passwords, or credentials unless expressly supported by a secure feature designed for that purpose.
13. Use bots, scripts, automated abuse, or excessive requests to degrade or manipulate the Services.
14. Attempt to extract prompts, model instructions, system architecture, scoring logic, proprietary datasets, or confidential platform methods.

We may suspend or terminate access for any suspected violation.

---

19. Responsible Security Use

The Services are intended for defensive and authorized security analysis. You may use the Services to review code that you own, control, are developing, are auditing with permission, or are otherwise authorized to test. You may not use the Services to facilitate unauthorized exploitation, theft, fraud, or attacks against third-party protocols, wallets, applications, users, networks, or systems. If you discover a vulnerability in third-party code, you are responsible for handling that information lawfully and ethically.

---

20. Account, Wallet, and Access Security

You are responsible for maintaining the security of any account, wallet, private key, API key, repository token, or credential used with the Services. We are not responsible for losses caused by:

- **Lost private keys**
- **Compromised wallets**
- **Unauthorized transactions**
- **Phishing**
- **User error**
- **Malware on your device**

- **Compromised API keys**
- **Unauthorized repository access**
- **Third-party wallet failures**

Notify us promptly if you believe your platform account or connected integration has been compromised.

---

21. Intellectual Property

The Services, including the website, software, user interface, platform design, prompts, scoring logic, model orchestration methods, report templates, branding, logos, trademarks, databases, workflows, algorithms, and documentation, are owned by us or our licensors and are protected by intellectual property laws. Subject to your compliance with these Terms, we grant you a limited, revocable, non-exclusive, non-transferable, non-sublicensable license to access and use the Services for their intended purpose. You may not copy, modify, distribute, sell, lease, reverse engineer, decompile, scrape, extract, or create derivative works based on the Services except as expressly permitted by law or written agreement.

---

22. Ownership of Reports

Unless otherwise agreed in writing, you may use Reports generated from your Submitted Materials for your internal development, remediation, compliance preparation, investor diligence, audit preparation, or related business purposes. You may share Reports with your team, contractors, auditors, investors, partners, or users at your discretion. However, you may not:

- Misrepresent the Report as a guarantee of security.
- Alter the Report in a misleading way.
- Use the Report to imply endorsement, certification, or approval by us.
- Remove disclaimers from the Report when publishing it publicly.
- Resell Reports as standalone audit products without permission.
- Claim that AI Consensus Audit has manually audited, certified, approved, or insured your code unless we expressly state so in writing.

---

23. Publicity and Use of Name

You may not use the name, logo, trademark, or branding of AI Consensus Audit, AIConsensusAudit.com, $AICA, or related marks in a way that implies partnership, endorsement, certification, sponsorship, or approval without our written permission. We may identify public projects that use the Services only where permitted by law and applicable privacy settings. If you require confidentiality, contact us before submitting materials or using the Services.

---

24. Third-Party Services

The Services may rely on or integrate with third-party services, including:

- **AI model providers**
- **Cloud infrastructure providers**
- **Wallet providers**
- **Blockchain networks**
- **Payment processors**
- **RPC providers**
- **Repository platforms**
- **Analytics providers**
- **Security tools**
- **Data providers**

We do not control third-party services and are not responsible for their availability, security, accuracy, failures, terms, policies, pricing, or conduct. Your use of third-party services may be subject to separate terms.

---

25. Beta Features and Experimental Tools

Some Services may be labeled beta, experimental, preview, early access, or similar. Beta features may be incomplete, unstable, inaccurate, unavailable, or changed without notice. You use beta features at your own risk. We may modify, suspend, discontinue, or limit beta features at any time.

---

26. Service Availability

We aim to provide reliable access, but we do not guarantee that the Services will be uninterrupted, error-free, secure, or available at all times. The Services may be unavailable due to:

- **Maintenance**
- **Model provider outages**
- **Cloud infrastructure issues**
- **Blockchain congestion**
- **Wallet failures**
- **Cyberattacks**
- **Network failures**
- **Software bugs**
- **Force majeure events**
- **Compliance or legal restrictions**

We are not liable for downtime, delays, failed scans, incomplete scans, or inability to access the Services.

---

27. Changes to the Services

We may modify, improve, suspend, limit, replace, or discontinue any part of the Services at any time. This includes changes to:

- **Scan pricing**
- **Supported chains**
- **Supported languages**
- **Model providers**
- **Report formats**
- **Risk scoring**
- **$AICA payment functionality**
- **API access**
- **Free scan limits**
- **Continuous re-scan features**
- **Token-related utilities**

We are not obligated to continue offering any specific feature indefinitely.

---

28. Disclaimer of Warranties

To the maximum extent permitted by law, the Services, Reports, website, APIs, token functionality, and all related materials are provided on an **"as is"** and **"as available"** basis. We disclaim all warranties, express or implied, including:

- **Merchantability**
- **Fitness for a particular purpose**
- **Non-infringement**
- **Accuracy**
- **Completeness**
- **Reliability**
- **Security**
- **Availability**
- **Error-free operation**
- **Detection of all vulnerabilities**
- **Suitability for deployment**
- **Regulatory compliance**
- **Compatibility with your systems**

We do not warrant that the Services will identify all vulnerabilities, prevent hacks, avoid financial loss, produce correct findings, or make any code secure.

---

29. Limitation of Liability

To the maximum extent permitted by law, AI Consensus Audit, its affiliates, founders, officers, directors, employees, contractors, agents, licensors, infrastructure providers, model providers, payment providers, and partners shall not be liable for any indirect, incidental, special, consequential, exemplary, enhanced, punitive, or similar damages, including:

- **Loss of funds**
- **Loss of tokens**
- **Smart-contract exploits**
- **Protocol hacks**
- **Lost profits**
- **Lost revenue**
- **Lost business opportunities**
- **Lost data**
- **Loss of goodwill**

- **Business interruption**
- **Cost of substitute services**
- **Deployment failures**
- **Third-party claims**
- **Security incidents**
- **Regulatory consequences**
- **Tax consequences**
- **Wallet compromise**
- **Blockchain transaction errors**

Whether based on warranty, contract, tort, negligence, strict liability, statute, or any other legal theory, even if we have been advised of the possibility of such damages. To the maximum extent permitted by law, our total aggregate liability for all claims arising out of or relating to the Services shall not exceed the greater of:

1. **The amount you paid to us for the specific scan giving rise to the claim**, or
2. **$100.**

Some jurisdictions do not allow certain limitations of liability, so some limitations may not apply to you.

---

30. Assumption of Risk

You acknowledge and accept the risks associated with:

- **Smart-contract development**
- **Blockchain deployment**
- **Crypto transactions**
- **AI-generated analysis**
- **Automated security tools**
- **Third-party infrastructure**
- **Model hallucinations**
- **False positives and false negatives**
- **Wallet use**
- **Token use**
- **Market and network volatility**
- **Regulatory uncertainty**
- **Open-source dependencies**
- **Protocol design flaws**

You assume full responsibility for all risks arising from your use of the Services.

---

31. Indemnification

You agree to defend, indemnify, and hold harmless AI Consensus Audit, its affiliates, founders, officers, directors, employees, contractors, agents, licensors, infrastructure providers, model providers, payment providers, and partners from and against any claims, damages, liabilities, losses, costs, and expenses, including reasonable attorneys' fees, arising out of or related to:

1. Your use or misuse of the Services.
2. Your Submitted Materials.
3. Your code, smart contracts, protocol, deployment, or users.
4. Your violation of these Terms.
5. Your violation of law or third-party rights.
6. Your unauthorized submission of code.
7. Your reliance on any Report.
8. Any exploit, loss, defect, or vulnerability in your code or protocol.
9. Your crypto transactions or wallet activity.
10. Your use, acquisition, transfer, or disposal of $AICA.
11. Any claim that your Submitted Materials infringe or misappropriate third-party rights.

We reserve the right to control the defense of any matter subject to indemnification, and you agree to cooperate with us.

---

32. Suspension and Termination

We may suspend, restrict, or terminate your access to the Services at any time, with or without notice, if we believe:

- You violated these Terms.
- Your use creates legal, security, operational, reputational, or compliance risk.
- Your activity is abusive, fraudulent, unlawful, or harmful.

- You are subject to sanctions or restricted jurisdiction rules.
- You attempted to exploit, disrupt, or reverse engineer the Services.
- Continued access is not commercially or technically feasible.

Upon termination, your right to use the Services ends immediately. Sections intended to survive termination will continue to apply, including disclaimers, payment obligations, intellectual property rights, limitation of liability, indemnification, dispute resolution, and governing law.

---

33. Modifications to These Terms

We may update these Terms from time to time. If we make material changes, we may provide notice by posting updated Terms on the website, updating the effective date, or using other reasonable methods. Your continued use of the Services after changes become effective means you accept the updated Terms. If you do not agree to updated Terms, stop using the Services.

---

34. Governing Law

These Terms shall be governed by and construed in accordance with the laws of **[Insert Governing Jurisdiction]**, without regard to conflict-of-law principles. You should select a governing jurisdiction after consulting legal counsel.

---

35. Dispute Resolution

Before filing any legal claim, you agree to first contact us at **[Insert Support Email]** and attempt to resolve the dispute informally. If the dispute cannot be resolved informally within **30 days**, the dispute shall be resolved through binding arbitration or courts located in **[Insert Venue/Jurisdiction]**, depending on the dispute-resolution structure selected by the company. If you want arbitration, use this version:**Binding Arbitration Option:**
Any dispute, claim, or controversy arising out of or relating to these Terms or the Services shall be resolved by final and binding arbitration administered by **[Arbitration Provider]** under its applicable rules. The arbitration shall take place in **[Location]**, be conducted in English, and be handled on an individual basis only. If you want court jurisdiction, use this version:**Court Venue Option:**
Any dispute arising out of or relating to these Terms or the Services shall be brought exclusively in

the state or federal courts located in **[Insert Venue]**, and you consent to personal jurisdiction and venue in those courts.

---

36. Class Action Waiver

To the maximum extent permitted by law, you and AI Consensus Audit agree that disputes shall be brought only on an individual basis. You waive any right to participate in a class action, collective action, representative action, private attorney general action, or consolidated proceeding.

---

37. Injunctive Relief

You acknowledge that unauthorized use, abuse, copying, reverse engineering, scraping, or disclosure of the Services, platform methods, proprietary systems, or confidential information may cause irreparable harm. We may seek injunctive or equitable relief without posting a bond, in addition to any other remedies available.

---

38. Force Majeure

We are not liable for delay or failure to perform caused by events beyond our reasonable control, including:

- Acts of God
- War
- Terrorism
- Civil unrest
- Government action
- Regulatory action
- Labor disputes
- Internet outages

- Cloud provider failures
- AI model provider failures
- Blockchain network failures
- Wallet provider failures
- Cyberattacks
- Natural disasters
- Power failures
- Pandemics
- Market disruption
- Other events beyond our control

---

39. Severability

If any provision of these Terms is found invalid, illegal, or unenforceable, the remaining provisions will remain in full force and effect. The invalid provision will be modified to the minimum extent necessary to make it enforceable, if permitted by law.

---

40. No Waiver

Our failure to enforce any provision of these Terms does not constitute a waiver of that provision or any other provision.

---

41. Assignment

You may not assign or transfer your rights or obligations under these Terms without our prior written consent. We may assign or transfer these Terms, in whole or in part, in connection with a merger, acquisition, restructuring, sale of assets, corporate transaction, or by operation of law.

42. Entire Agreement

These Terms, together with any incorporated policies or additional written agreements, constitute the entire agreement between you and AI Consensus Audit regarding the Services and supersede all prior or contemporaneous agreements, communications, or understandings.

---

43. Contact

For questions about these Terms, contact:**AI Consensus Audit**
Website: **AIConsensusAudit.com**
Email: **[Insert Support Email]**
Legal Contact: **[Insert Legal Email]**
Company: **[Insert Company Legal Name]**
Address: **[Insert Company Address]**

Suggested Short Footer Disclaimer

You may also want this in the site footer:**AIConsensusAudit.com provides AI-assisted smart-contract security analysis. Reports may contain errors, omissions, false positives, or false negatives and do not guarantee that code is secure. Full scans are $100, or $50 when paid with $AICA$. AICA is a utility token for platform access and payment; it does not represent equity, revenue share, profit rights, or investment rights.**

Suggested Checkout Checkbox Text

Use this before a user pays: **By purchasing a scan, I agree to the Terms of Service and understand that AI Consensus Audit provides AI-assisted analysis only. Reports may contain errors or omissions and do not guarantee code security. Crypto payments are final once processing begins.**