TAUTH LABS, INC.
SUBSCRIBER AGREEMENT

This Subscriber Agreement (this "Agreement") is a binding contract between Tauth Labs, Inc., acting in its capacity as a C2PA-conformant Certification Authority ("Tauth," the "CA," "we," or "us"), and the individual or legal entity that applies for, accepts, or uses any Certificate issued by the CA (the "Subscriber" or "you").

PLEASE READ THIS AGREEMENT CAREFULLY. BY SUBMITTING A CERTIFICATE APPLICATION, OR BY ACCEPTING OR USING ANY CERTIFICATE ISSUED BY THE CA, THE SUBSCRIBER CONFIRMS THAT IT HAS READ AND UNDERSTOOD THIS AGREEMENT AND AGREES TO BE BOUND BY IT. IF THE SUBSCRIBER DOES NOT AGREE, IT MUST NOT APPLY FOR, ACCEPT, OR USE ANY CERTIFICATE. QUESTIONS REGARDING THIS AGREEMENT MAY BE DIRECTED TO THE CA AT CA@TAUTH.IO.

1. DEFINITIONS

Capitalized terms not defined elsewhere in this Agreement have the meanings below. Terms defined in the CP/CPS or the C2PA Specifications carry those meanings when used here in a certification context.

"Application" means a Certificate request submitted by the Subscriber, comprising a Certificate Signing Request (CSR) together with the identity, organization, and product information required under the CP/CPS.

"Assurance Level" means the level of identity and key-protection assurance assigned to a Certificate under the CP/CPS and the applicable C2PA requirements.

"C2PA Requirements" means, collectively, the current approved versions of the C2PA technical specifications, the C2PA Certificate Policy, and the C2PA conformance requirements applicable to generator products, each as published by the Coalition for Content Provenance and Authenticity and amended from time to time.

"Certificate" means a digital certificate issued to the Subscriber by the CA under this Agreement, binding a Public Key to the Subscriber's validated identity.

"Conforming Products List" means the public register of generator products that have completed the C2PA conformance program.

"CP/CPS" means the Tauth Labs Certificate Policy and Certification Practice Statement, structured in accordance with RFC 3647 and published in the CA's public repository, as amended from time to time.

"Generator Product" means the hardware or software product, identified in the Application, that assembles and signs C2PA manifests using the Certificate.

"Key Compromise" means any loss, theft, unauthorized disclosure, unauthorized use, or modification of a Private Key, or any other event that undermines confidence in the exclusivity of the Subscriber's control over that key.

“Key Pair” means a Private Key and its mathematically related Public Key.

“Manifest” means a C2PA manifest: a set of cryptographically bound assertions describing the provenance of a digital asset.

“Private Key” means the secret component of a Key Pair, which must remain under the Subscriber’s exclusive control unless the Subscriber uses the CA’s managed key service.

“Public Key” means the publicly disclosable component of a Key Pair that is embedded in a Certificate.

“Relying Party” means any person or entity that relies on a Certificate, a Manifest signed under a Certificate, or certificate status information published by the CA.

“Repository” means the CA’s publicly accessible collection of governing documents and certificate status services, including CRLs and OCSP responders.

“Trustworthy System” means hardware, software, and operational procedures that are reasonably protected against intrusion and misuse, operate with a reasonable level of availability and reliability, and are appropriate for the functions they perform.

2. GOVERNING DOCUMENTS

2.1. Incorporation by Reference. The CP/CPS and the applicable C2PA Requirements are incorporated into this Agreement by reference. Where this Agreement and the CP/CPS conflict on a matter of certificate lifecycle practice, the CP/CPS controls; where they conflict on a commercial matter, this Agreement controls, subject to Section 8 of the Master Services Agreement where applicable.

2.2. Amendments. The Subscriber acknowledges that the CA must maintain conformance with evolving C2PA and industry standards, and agrees that the CA may amend the CP/CPS and this Agreement from time to time for that purpose. Amendments become effective upon publication in the Repository. The Subscriber’s continued use of a Certificate after publication constitutes acceptance; if the Subscriber does not accept an amendment, its sole remedy is to request revocation of its Certificates and cease use.

3. APPLICATION, VALIDATION, AND ISSUANCE

3.1. Application. The Subscriber may apply for Certificates by submitting an Application through the channels described in the CP/CPS. By submitting an Application for a claim-signing Certificate, the Subscriber represents that the identified Generator Product appears on the Conforming Products List, or is the subject of a pending conformance application disclosed to the CA, and that the Subscriber will not place the Certificate into production use before conformance is confirmed.

3.2. Validation and Discretion to Issue. The CA will validate each Application in accordance with the CP/CPS, including verification of the Subscriber’s identity and its authority over any organization name or product identified in the Application. Issuance is at the CA’s discretion; the CA may decline any Application, including where the Generator Product does not satisfy applicable C2PA security requirements, without incurring liability, and will refund any prepaid issuance fee for a declined Application.

3.3. Certificate Acceptance. A Certificate is deemed accepted upon the earlier of: (a) the Subscriber's first use of the Certificate; or (b) fifteen (15) days after issuance, unless the Subscriber notifies the CA of an error in the Certificate within that period.

4. LICENSE AND PERMITTED USES

4.1. License. Effective upon issuance and continuing until the Certificate expires or is revoked, the CA grants the Subscriber a limited, non-exclusive, non-transferable, revocable license to use the Certificate within a Trustworthy System, solely for the uses permitted under this Section 4 and the key usage and extended key usage fields encoded in the Certificate itself.

4.2. Claim-Signing Certificates. A claim-signing Certificate may be used only to sign Manifests generated by verified instances of the Generator Product identified in the Application. The Subscriber shall ensure that the Generator Product's deployed implementation continues to match the design, specifications, and security controls presented during conformance evaluation, including maintaining a faithful correspondence between the content presented to end users and the content cryptographically bound within the Manifest.

4.3. Identity Certificates. An identity Certificate may be used only to assert the identity of the Subscriber as validated by the CA. The Subscriber shall not use an identity Certificate to sign on behalf of, or to attribute content to, any other person or entity.

4.4. Timestamping. Where the Subscriber's use of the Service involves trusted timestamps, such use must conform to RFC 3161, the timestamping provisions of the C2PA Requirements, and the operational requirements of the CP/CPS.

4.5. Prohibited Uses. The Subscriber shall not use any Certificate, or permit any Certificate to be used, to sign content or provenance data that:

(a) contains provenance assertions the Subscriber knows or reasonably should know to be false, fabricated, or materially misleading;

(b) facilitates unlawful activity, incites violence, constitutes hate speech, or comprises intimate or sexual imagery of any person who has not consented to its creation and distribution;

(c) falsely implies that a third party created, endorsed, or is affiliated with the signed content, absent that party's written authorization; or

(d) is otherwise prohibited under the CP/CPS or the CA's published acceptable use policy.

5. SUBSCRIBER OBLIGATIONS

5.1. Truthful Information. All information the Subscriber provides to the CA — in an Application, during validation, or otherwise — must be accurate, current, and complete. The Subscriber shall notify the CA promptly, and in any event within seven (7) days, of any change that makes previously provided information inaccurate, including changes of legal name, control of the organization, or ownership of the Generator Product.

5.2. Truthful Assertions. The Subscriber is solely responsible for the truthfulness and accuracy of every assertion, claim, and item of metadata embedded in content signed under its Certificates.

5.3. Key Generation and Protection. Unless the Subscriber uses the CA's managed key service, the Subscriber shall: (a) generate its Key Pairs using algorithms and parameters approved under the CP/CPS; (b) store and operate each Private Key within a Trustworthy System that meets or exceeds the protections required for the Certificate's Assurance Level; and (c) restrict access to Private Keys to personnel with a demonstrated need. As between the parties, the Subscriber bears sole responsibility for any Key Compromise affecting keys under its control.

5.4. Monitoring and Abuse Detection. The Subscriber shall maintain reasonable procedures to monitor signing activity under its Certificates, including detection of anomalous signing volumes, unauthorized use of the Generator Product, and indications of Key Compromise.

5.5. Incident Notification. If the Subscriber suspects or discovers a Key Compromise, a security vulnerability affecting the Generator Product, a material data quality defect in signed Manifests, or any violation of this Agreement, the Subscriber shall immediately suspend use of the affected Certificate and notify the CA within twenty-four (24) hours, and shall thereafter cooperate with the CA's investigation and remediation efforts.

5.6. Revocation Status Handling. The Subscriber shall integrate certificate status checking in the manner recommended by the C2PA Requirements and the Documentation, including embedding OCSP responses into Manifests at signing time and caching status responses so that the Generator Product does not query the CA's status services on every signing event. For sustained high-volume signing (in excess of one million signing operations per calendar month) conducted without these measures, the CA reserves the right to assess a reasonable infrastructure surcharge as published in its fee schedule or the applicable Order Form.

5.7. Cessation After Expiry or Revocation. Upon expiration or revocation of a Certificate, the Subscriber shall immediately cease all signing with that Certificate and its associated Private Key, and shall not attempt to circumvent revocation through timestamp manipulation or otherwise.

6. REVOCATION

6.1. Revocation by the CA. The CA may revoke a Certificate, with notice where practicable but without prior notice where circumstances require, if the CA reasonably determines that:

(a) the Subscriber has materially breached this Agreement, the CP/CPS, or the acceptable use provisions of Section 4.5;

(b) the Private Key has suffered a Key Compromise or is not maintained within a Trustworthy System;

(c) the Generator Product has been removed or suspended from the Conforming Products List, or no longer conforms to the version evaluated;

(d) any information in the Certificate is, or has become, inaccurate or misleading;

(e) revocation is required under the CP/CPS, the C2PA Requirements, or applicable law; or

(f) revocation is reasonably necessary to protect the integrity of the CA's trust infrastructure, Relying Parties, or the broader content provenance ecosystem.

6.2. Revocation on Request. The Subscriber may request revocation of its own Certificates at any time through the authenticated channels described in the CP/CPS, and shall do so promptly upon any Key Compromise.

6.3. No Refund on Revocation for Cause. Fees attributable to a Certificate revoked due to the Subscriber's breach or Key Compromise are non-refundable.

7. FEES

7.1. Fees. The Subscriber shall pay the fees stated in the applicable Order Form or, where no Order Form applies, the CA's published fee schedule. Payment terms are as stated in the Master Services Agreement, where one is in effect between the parties.

7.2. Taxes. Fees are exclusive of taxes, duties, and levies, all of which are the Subscriber's responsibility, other than taxes on the CA's net income.

8. INTELLECTUAL PROPERTY

8.1. CA Materials. The CA and its licensors retain all right, title, and interest in and to the Certificates as issued artifacts (excluding Subscriber information contained within them), the Repository contents, certificate status data (including CRLs and OCSP responses), the CA's signing infrastructure, and the Documentation.

8.2. Subscriber Materials. The Subscriber retains all right, title, and interest in and to its Private Keys, its content, and any trademarks, trade names, or organizational identifiers included in a Certificate's subject information at the Subscriber's request.

9. WARRANTIES AND DISCLAIMERS

9.1. CA Warranty. The CA warrants to the Subscriber that, at the time of issuance: (a) the Certificate was issued in material conformance with the CP/CPS; and (b) the CA had no actual knowledge of any material misrepresentation of fact contained in the Certificate.

9.2. Subscriber Warranties. The Subscriber represents and warrants, for the benefit of the CA and each Relying Party, that: (a) it holds all rights necessary to use the Generator Product and to sign the content it signs; (b) it will protect its Private Keys as required by Section 5.3; (c) each provenance assertion made under its Certificates is truthful; and (d) it will use Certificates only as permitted by Section 4.

9.3. DISCLAIMER. EXCEPT FOR THE EXPRESS WARRANTY IN SECTION 9.1, ALL CERTIFICATES AND RELATED SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE." THE CA DISCLAIMS ALL OTHER WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. THE CA DOES NOT WARRANT UNINTERRUPTED OR ERROR-FREE OPERATION OF ITS SERVICES, NOR THAT ANY THIRD-PARTY PLATFORM WILL RECOGNIZE, DISPLAY, OR HONOR ANY CERTIFICATE OR MANIFEST.

10. INDEMNIFICATION

The Subscriber shall defend, indemnify, and hold harmless the CA, its affiliates, and their respective directors, officers, employees, and agents, together with Relying Parties and application software vendors that rely on the CA's certificates (collectively, the "Indemnified Parties"), from and against any claims, damages, liabilities, costs, and expenses (including reasonable attorneys' fees) arising out of or relating to:

(a) the Subscriber's breach of this Agreement or of any warranty in Section 9.2;

(b) any false or misleading statement made by the Subscriber in an Application or embedded in signed content;

(c) any Key Compromise of a Private Key under the Subscriber's control, or the Subscriber's failure to request timely revocation following such a compromise; or

(d) any allegation that the Subscriber's use of a Certificate infringed the rights of a third party or authenticated unlawful or harmful content.

11. CONFIDENTIALITY AND PUBLICATION

11.1. Validation Materials. Information the CA collects from the Subscriber during identity, organization, or product validation that is not included in an issued Certificate or otherwise published will be treated as the Subscriber's confidential information and handled in accordance with the CP/CPS and, where applicable, Section 5.4 of the Master Services Agreement.

11.2. Public Records. The Subscriber acknowledges that issued Certificates and certificate status information are, by design, public artifacts of a trust infrastructure, and consents to their publication and distribution by the CA through the Repository, CRLs, OCSP services, and any applicable transparency mechanisms.

12. TERM AND TERMINATION

12.1. Term. This Agreement takes effect on the date the Subscriber first submits an Application or accepts a Certificate, whichever occurs first, and remains in effect until the last Certificate issued under it expires or is revoked, unless terminated earlier.

12.2. Termination for Breach. Either party may terminate this Agreement upon written notice if the other party materially breaches it and fails to cure the breach within thirty (30) days of notice; provided that the CA's revocation rights under Section 6 operate independently of, and are not delayed by, this cure period.

12.3. Effect of Termination; Survival. Upon termination, all Certificate licenses end and the CA may revoke outstanding Certificates. Sections 5.7, 6, 8, 9, 10, 11, 12.3, and 13 survive termination, together with any accrued payment obligations.

13. GENERAL

13.1. Governing Law and Venue. This Agreement is governed by the laws of the State of New York, without regard to its conflict of laws principles. The parties submit to the exclusive jurisdiction of the state and federal courts located in New York, New York.

13.2. Relationship to Other Documents. This Agreement, together with the CP/CPS, the applicable Order Form, and (where in effect) the Master Services Agreement, constitutes the entire agreement between the parties concerning Certificates and supersedes all prior agreements on that subject. The limitation of liability framework set forth in Section 8 of the Master Services Agreement applies to claims arising under this Agreement.

13.3. Third-Party Beneficiaries. Relying Parties and application software vendors that rely on the CA's certificates are intended third-party beneficiaries of the Subscriber's representations, warranties, and indemnification obligations under this Agreement. No other person has any rights under this Agreement.

13.4. Assignment. The Subscriber may not assign this Agreement, or transfer any Certificate, without the CA's prior written consent. Any purported assignment in violation of this Section is void.

13.5. Notices. Notices to the CA must be sent to ca@tauth.io or to such other contact address as the CA publishes in the Repository. Notices to the Subscriber may be sent to the contact information provided in the most recent Application, which the Subscriber is responsible for keeping current.

13.6. Severability; Waiver. If any provision of this Agreement is held invalid or unenforceable, it will be reformed to the minimum extent necessary to make it enforceable, and the remainder of the Agreement will continue in full force. A party's failure to enforce any provision is not a waiver of its right to do so later.

Version 1.0 – July 2026