CISA Secure by Design Pledge Statement

CISA

TROOTH, LLC CERT-001

Document Title	CISA Secure by Design Pledge Statement
Document ID	CERT-001
Version	2.0
Classification	Public
Effective Date	September 18, 2026
Next Scheduled Review	March 18, 2027
Document Owner	D'Andre Heggie, Founder and Sole Member
Entity	Trooth, LLC
Supersedes	CISA Secure by Design Public Pledge Statement 1.0, June 8, 2026 (signed)
Reference Frameworks	CISA Secure by Design Pledge (seven goals)

1. Executive summary

Trooth, LLC signed the Secure by Design Pledge published by the United States Cybersecurity and Infrastructure Security Agency. The Pledge asks a software manufacturer to make measurable progress against seven goals within a year and to publish what it did. This statement records the Company's position against each of the seven, including the two where the honest answer is that the work is not finished. Signing the Pledge is a voluntary public undertaking; CISA does not audit signatories and the Pledge is not a certification.

2. Scope

Trooth, LLC (the Company) operates one product: the Trooth Network, a web application at trooth.co with a public API at api.trooth.co. A company connects its systems, the Network records what is true of them on a schedule with the source and the time of each observation, and buyers read that record. This statement covers that product, the production database that

holds its data, the deployment pipeline that builds it, and the administrative accounts the Company holds with each provider named in its published Sub-processor List. It does not cover preview or development environments, which hold no customer data. As at the effective date the Company has no employees or contractors; every requirement written for personnel applies to the Founder today and to every future person from their first day.

3. The seven goals

Goal	Position on the effective date
1. Multi-factor authentication	MET. Authenticator-app multi-factor authentication is built in and free for every account, including buyer accounts, and is never a paid feature. GAP: the authentication service offers no recovery or backup codes, so an account that loses its authenticator relies on a manual recovery path. The Trust Center states that control as not in place and the test suite asserts the absence rather than papering over it.
2. Default passwords	MET. The product ships no default password. There is no shared, seeded or vendor-set credential of any kind: every account is created by the person who will use it, and every administrative credential is unique and held in a secret store.
3. Reducing entire classes of vulnerability	MET, and enforced in the build. Whole classes are removed by construction rather than by review: parameterised queries throughout, so injection has no surface; a content security policy minted per request with a nonce and no inline script, so cross-site scripting has nowhere to run; row-level security in the database under a role that cannot bypass it, so a missed check in application code still cannot cross a tenant boundary; request bodies parsed against declared schemas, so mass assignment is impossible; and authorization derived from the session and never from the request body. One hundred and fifty-two automated gates check these on every change and a failing gate stops the deploy.
4. Security patches	MET. Dependencies are watched by Dependabot, audited for high and critical advisories on every push, and static analysis runs on every push. The published Vulnerability Management Policy (POL-07) sets remediation at 24 hours for a critical finding in production, 7 days for high, 30 for medium and 90 for low. Deployment is a single automated path from the main branch, so a patch reaches production in minutes rather than waiting for a release window.
5. Vulnerability disclosure policy	MET. A policy is published at trooth.co/security/vulnerability-disclosure-policy with scope, expectations and an explicit safe harbour for good-faith research, and security.txt at the standard well-known location points to the same address. Reports go to security@trooth.co and a person answers.

Goal	Position on the effective date
6. CVE transparency	PARTIALLY MET. The Company has issued no CVE because no vulnerability in its own software has met the threshold; it commits to issuing one with an accurate CWE field if that changes. GAP: the software bill of materials served at /sbom.json describes the platform Workers as of 23 July 2026 rather than the current web application. The Trust Center states that control as not in place; it becomes attested when the generated file is live.
7. Evidence of intrusions	MET. Material actions in the product are written to an append-only, hash-linked audit ledger whose chain is verified by a build gate, so a removed or altered entry is detectable. Customers can see the ledger for their own workspace. Application errors are captured with personal data removed before an event leaves the server; platform request logs, deploy history and provider audit logs are retained as ATT-01 describes; and availability is watched from outside and published at trooth.co/status.

4. Scope of the pledge

This pledge applies to Trooth, LLC and to the software it develops and operates: the Trooth Network at trooth.co, its public API at api.trooth.co, and any product or service the Company releases in future. The Company operates no other software product on the effective date. Where a goal is met by a control the Company inherits from a provider rather than implements itself, this statement says so rather than claiming the provider's work as its own.

5. What this pledge is not

The Secure by Design Pledge is a voluntary commitment. CISA publishes the roster of signatories; it does not assess, test, audit or endorse any signatory, and signing confers no approval, authorisation or certification. The Company holds no audited certification against any framework. The two gaps named in section 3 are stated here for the same reason they are stated on the Trust Center: a pledge that reported only the goals already met would not be worth reading.

Reference: CISA Secure by Design Pledge, seven goals. Related: POL-03 Password and Authentication; POL-06 Secure Development and Change Management; POL-07 Vulnerability Management; POL-08 Logging, Monitoring and Access Review; ATT-01; trooth.co/security/vulnerability-disclosure-policy; trooth.co/.well-known/security.txt; trooth.co/status.

Authorization

This statement is issued by Trooth, LLC under the authority of its Founder and Sole Member and describes the Company as it operates on its effective date. It is a published statement of the Company and requires no signature to bind it; the version published at trooth.co/security

is the current one, and an earlier version, including any signed version of June 8, 2026, is superseded in full. It is not a certification and not an audit opinion: Trooth holds no audited certification against any framework and does not represent otherwise. Where this statement and the live service disagree, the service is corrected or the statement is re-issued, and the Company's published Trust Center states, control by control, what is in place and what is not.