NIST Cybersecurity Framework 2.0 Profile

NIST CSF 2.0

TROOTH, LLC NIST-CSF-2026-001

Document Title	NIST Cybersecurity Framework 2.0 Profile
Document ID	NIST-CSF-2026-001
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	NIST Cybersecurity Framework 2.0 Profile 1.0, June 8, 2026 (signed)
Reference Frameworks	NIST Cybersecurity Framework 2.0 (February 2024)

1. Executive summary

This is Trooth, LLC's current profile against the six functions of the NIST Cybersecurity Framework 2.0, written by the Founder. It states, function by function, the outcomes the Company achieves and the ones it does not yet, and it names the evidence for each: a file, a build gate, a workflow run, a published document or a header any reader can fetch. It is a self-assessment and not a certification; NIST certifies no one and issues no badge, and the Company holds no audited certification against any framework.

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. GOVERN (GV)

Outcome	Position and evidence
Organizational context (GV.OC)	ACHIEVED. The Company operates one product for a defined set of customers and buyers; the mission, the dependencies and the legal obligations that bear on it are written in POL-01 and in the published Trust Center.
Risk management strategy (GV.RM)	ACHIEVED. POL-13 sets how risk is identified, scored, treated and reviewed; the risk register records each risk with the control and the evidence, and is re-read whenever the gate list or the known-limitations record changes.
Roles, responsibilities and authorities (GV.RR)	ACHIEVED for the present shape. The Founder owns every security decision and holds the only production write access; POL-01 section 4 names what a future person and a sub-processor are each accountable for.
Policy (GV.PO)	ACHIEVED. Nineteen policies, POL-01 to POL-19, are published with an owner, an effective date and a six-month review date, and take effect as published statements of the Company.
Oversight (GV.OV)	PARTIALLY ACHIEVED. Review is scheduled and the outcomes of the build gates are visible on every change, but the Company has no board, no independent reviewer and no external audit; oversight is the Founder reviewing the Founder, and this profile says so.
Cybersecurity supply chain risk management (GV.SC)	PARTIALLY ACHIEVED. Every sub-processor is engaged under a written agreement, published with purpose and region, and reviewed under POL-14; build inputs install from a frozen lockfile and every third-party build action is pinned to a full commit hash. GAP: the published software bill of materials describes the platform Workers rather than the web application.

4. IDENTIFY (ID)

Outcome	Position and evidence

Outcome	Position and evidence
Asset management (ID.AM)	ACHIEVED. Inventories of external services, information assets by classification, routes, components and public files; the generated ones are regenerated from source and compared on every build, so an undocumented asset fails the deploy.
Risk assessment (ID.RA)	PARTIALLY ACHIEVED. Dependency advisories and static analysis run on every push; the risk register is maintained. GAP: no independent penetration test has been performed, which this category expects; the engagement is deferred until the first enterprise customer and the Trust Center states it.
Improvement (ID.IM)	ACHIEVED. Every finding, its cause and its fix are recorded in a public register; the practice of turning a finding into a build gate rather than a note is how most of this document's evidence came to exist.

5. PROTECT (PR)

Outcome	Position and evidence
Identity management, authentication and access control (PR.AA)	PARTIALLY ACHIEVED. Multi-factor authentication is available to every account and required on every provider account the Company holds; sessions are httpOnly, secure, same-site with a fixed expiry; authorization is derived from the session and checked by a build gate. GAPS: no multi-factor recovery codes, and the first ninety-day access review has not yet been recorded.
Awareness and training (PR.AT)	NOT YET ACHIEVED. POL-16 requires training within thirty days of access and annually; no completion record exists. Target: 31 October 2026.
Data security (PR.DS)	ACHIEVED. TLS 1.2 or 1.3 in transit with HSTS preloaded; AES-256 at rest in the managed database and its backups; the Company's own nightly export encrypted before it leaves the runner; tenant separation enforced twice and proven live. Detail in ATT-02 and ATT-03.
Platform security (PR.PS)	ACHIEVED. One path to production through one hundred and fifty-two gates; a content security policy minted per request with a nonce; security headers set per prefix so two headers cannot disagree; secrets held in platform stores and scanned for on every commit and every push.
Technology infrastructure resilience (PR.IR)	ACHIEVED. One public port; the database reachable only over TLS with credentials from the application; production separated from preview and development by host, configuration and data; recovery objectives of four hours to restore and twenty-four hours of maximum data loss.

6. DETECT (DE)

Outcome	Position and evidence
Continuous monitoring (DE.CM)	ACHIEVED for the surfaces that exist. External monitors check the site, the API and the health route on a schedule and publish to a public status page; errors are captured with personal data removed before an event leaves the server; edge rules block and log at the network layer; the audit-ledger chain is verified on every build. DE.CM-02, physical environment monitoring, is not applicable: the Company operates no premises.
Adverse event analysis (DE.AE)	PARTIALLY ACHIEVED. Signals are correlated by hand by the Founder against the ledger, the error stream and the platform logs. There is no security information and event management system and no automated correlation, and at this size the Company judges a tool it cannot tune to be worse than the attention it would replace. This profile states the position rather than implying a capability.

7. RESPOND (RS) and RECOVER (RC)

Outcome	Position and evidence
Incident management, analysis, reporting and mitigation (RS.MA, RS.AN, RS.CO, RS.MI)	PARTIALLY ACHIEVED. POL-09 sets four severities with first response from fifteen minutes, covers containment, eradication and recovery, commits to the status page immediately and to customer email within seventy-two hours where personal data is affected, and requires a written post-mortem for the two highest severities. GAP: the plan has not been exercised in a drill; the first is scheduled.
Incident recovery plan execution and communication (RC.RP, RC.CO)	ACHIEVED. Nightly encrypted backups with a monthly restore rehearsal that checks the tables, the row security and the row counts on the restored database; the first rehearsal completed on 10 September 2026. The deploy's own smoke promotes the previous deployment back on failure. Recovery communication runs through the public status page, which anyone can subscribe to.

8. The profile in one paragraph

Twelve of the nineteen categories assessed are achieved, six are partially achieved and one is not yet achieved. Every shortfall traces to one of six things the Trust Center already names as controls not in place: no training record, no recorded access review, no incident-response drill, no independent penetration test, no current software bill of materials for the web application, and no multi-factor recovery codes. There is no seventh gap hiding in this document. The Company publishes no Tier rating under the Framework's implementation scale, because a rating an organisation assigns to itself, with no assessor and no evidence requirement behind it, tells a buyer less than the table above.

Reference: NIST Cybersecurity Framework 2.0, February 2024, functions GOVERN, IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER. Related: POL-01; POL-07; POL-08; POL-09; POL-10; POL-11; POL-13; POL-14; POL-16; ATT-01; ATT-02; ATT-03; ATT-04; trooth.co/security; 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.