Climate Data Governance Framework

CleantechHUB's operating constitution for sovereign climate data governance in Latin America.

- Framework Overview
- Constitutional Layer
  - CTH as Framework Operator
  - Governance Board
  - Dispute Resolution & Framework Evolution
- Roles & Permissions
  - Role Taxonomy Overview
  - Data Submitter
  - Accredited Validator
  - Community Sovereign
  - CTH Data Steward
  - Regulator / Auditor
  - AI Agent
- Decision Rules
  - R-SUB: Submission Rules
  - R-VAL: Validation Rules
  - R-CON: Consent & Benefit Rules
  - R-AGT: Agent Rules
  - R-CHG: Change Governance Rules
- Technical Standards Stack
  - Standards Overview
  - T-01: Identity & Credential Layer
  - T-02: Provenance & Quality Layer
  - T-03: Policy & Enforcement Layer

    - T-04: Discovery & AI Access Layer

- Regulatory Mappings
    - EUDR — EU Deforestation Regulation
    - CSRD — Corporate Sustainability Reporting
    - CBAM — Carbon Border Adjustment Mechanism
    - ISSB IFRS S2 — Climate Disclosures
    - Article 6.4 — Paris Agreement Carbon Credits

Framework Overview

Climate Data Governance Framework

CleantechHUB's operating constitution for sovereign climate data in Latin America

Version 1.0 · May 2026 · CC-BY 4.0

This framework governs how climate data is collected, validated, consented, stored, and used across CleantechHUB's programmes and partner networks. It applies to all data that flows through CTH's infrastructure — from KoboToolbox field surveys in Colombian coffee regions to CBAM-compliant emissions records for LATAM exporters.

? Related: Sovereign Climate Data — 10 Principles — the normative principles this framework operationalises. The governance framework is the *operating constitution*; the principles are the *substantive standards*.

Framework Structure

?? 1 — Constitutional Layer

CTH as Framework Operator. Governance board composition. Voting, dispute resolution and framework evolution.

? 2 — Roles & Permissions

Six roles: Data Submitter, Accredited Validator, Community Sovereign, CTH Data Steward, Regulator/Auditor, AI Agent.

? 3 — Decision Rules

15 machine-executable rules across five domains: submission, validation, consent, AI agents, and framework changes.

? 4 — Technical Standards Stack

Seven-layer architecture: DID ? VC ? PROV-O ? Ledger ? ODRL/OPA ? DCAT ? Compliance outputs.

? 5 — Regulatory Mappings

EUDR (Dec 2026), CSRD ESRS E1/E4, CBAM (Sep 2027), ISSB IFRS S2, Article 6 Paris Agreement.

Design Principles

Principle	What it means
Operator ? Owner	CTH operates the infrastructure but does not own or control the data. Analogous to ICANN for DNS.
Consent is structural	FPIC checks are enforced at database level — no role, including CTH, can bypass them.
Agents are first-class	AI agents have explicit permissions, mandatory audit logging, and must pass a policy check before every write.
Rules are executable	All decision rules are encoded as ODRL policies enforced by OPA — not prose guidelines.
Compliance is output, not goal	EUDR, CSRD, CBAM compliance reports are generated automatically from the governance ledger — not assembled manually.

Framework version 1.0 · Published May 2026 · CleantechHUB · Licence: CC-BY 4.0 · Governed under: This framework

Constitutional Layer

Constitutional Layer

CTH as Framework Operator

CTH as Framework Operator

CleantechHUB operates the infrastructure. It does not own the data.

Constitutional Layer · C-01

The most important design choice in this framework: **CTH is the operator, not the owner.** CTH maintains the technical infrastructure, publishes the standards, certifies validators, and enforces the rules. CTH does not own, sell, or unilaterally access the climate data that flows through the system.

The ICANN Model: ICANN operates the Domain Name System globally. It maintains the protocol, accredits registrars, and enforces policy. It does not own domain names — registrants do. CTH's relationship to climate data is structurally identical. CTH maintains the protocol and enforces the framework; data submitters and communities own their data.

What CTH Can Do

? Maintain infrastructure

Operate the governance ledger, API, and credential verification services.

? Publish standards

Release new framework versions, SHACL shapes, and methodology registries.

? Certify validators

Issue CTH Validator Credentials to organisations meeting EN ISO/IEC 14065 requirements.

? Enforce submission rules

Reject submissions that fail SHACL validation or lack required FPIC credentials.

What CTH Cannot Do

? Override FPIC consent

CTH cannot access community-restricted data even with full administrator credentials. This is enforced at database row-level security — not policy.

? Sell or license data

CTH cannot sell, license, or grant access to data it does not own. Data owners control their own ODRL usage policies.

? Change framework unilaterally

Major framework changes require a ? board supermajority. Changes touching FPIC rules additionally require Community Sovereignty Panel affirmative vote.

? Validate its own data

CTH-submitted data must be validated by a third-party accredited validator. No self-certification.

Legal Basis

Jurisdiction	Relevant instrument	Implication for CTH
Colombia	Law 21 of 1991 (ILO 169 ratification)	Free Prior and Informed Consent mandatory before collecting data in indigenous territories
Colombia	2016 Peace Accords — Ethnic Chapter	Community data rights recognised as part of territorial rights
EU	GDPR Article 5	Data minimisation and purpose limitation — encoded in ODRL policies
Brazil	LGPD (Lei 13.709/2018)	Consent requirements for personal data in emissions records
International	CARE Principles (GIDA 2018)	Collective benefit, authority to control, responsibility, ethics — all encoded in framework rules

Constitutional Layer

Governance Board

Governance Board

Multi-stakeholder deliberation body. No single constituency can dominate.

Constitutional Layer · C-02

The Governance Board makes decisions about the framework itself — what rules apply, which methodologies are accepted, how disputes are resolved. CTH holds one seat as Operator but cannot outvote the other four seats combined. The board structure is designed to prevent regulatory capture.

Board Composition

? Scientific Council

Members: IDEAM, CGIAR/CIAT, national universities (UNAL, Los Andes), independent climate scientists.

Authority: Approves and rejects methodologies. Arbitrates technical disputes. Maintains the methodology registry.

? Community Sovereignty Panel

Members: COICA (pan-Amazonian), Arhuaco, Wayúu, farmer cooperative representatives (Federacafé regional).

Authority: Veto on any rule touching FPIC, indigenous data rights, or benefit-sharing. Arbitrates consent disputes.

? Industry Council

Members: LATAM exporters, EU commodity importers, certification bodies, commodity traders.

Authority: Tests practical workability of rules. Shapes usability and adoption. Cannot set rules against community interests.

? Civil Society Seat

Members: Environmental NGOs, Global Forest Watch, Rainforest Alliance technical staff, Colombian environmental watchdogs.

Authority: Anti-capture guarantee. Can publicly dissent from any board decision and trigger a 30-day review.

?? Regulatory Observers

Members: EU DG ENV, Colombia MinAmbiente, Brazil IBAMA, Mexico SEMARNAT.

Authority: Observer only — no voting rights. Must be notified of material framework changes within 30 days.

Voting Rules

Decision type	Required majority	Additional conditions
Major version change (new principles, breaking schema changes)	? of all seats	30-day public comment period. Minimum 4/5 seats must vote (quorum).
Minor version change (new accepted methodology, optional field)	Simple majority	14-day comment period. CTH operator decision with board notification.
Any rule touching FPIC or indigenous data rights	? of all seats *plus* affirmative Community Panel vote	Community Panel veto is structural — not procedural. Board supermajority alone is insufficient.
Validator accreditation / de-accreditation	Scientific Council recommendation + CTH Steward decision	No full board vote required unless disputed.
Emergency patch (security / data integrity)	CTH Operator alone	48h notification to all seats. Board ratification within 30 days or auto-rollback.

Decision Log

All board decisions are published in the framework's decision log within 7 days of vote. Individual seat votes are visible — no anonymous voting. The decision log is stored as an append-only series of governance events in the governance ledger, signed by each voting DID.

Dispute Resolution & Framework Evolution

Dispute Resolution & Framework Evolution

How contested data is handled. How the framework itself grows.

Constitutional Layer · C-03

Dispute Resolution

Two types of disputes require different arbitration tracks.

? Technical Disputes

Example: Is a satellite imagery dataset authoritative for the 2020 deforestation baseline? Is methodology X equivalent to GHG Protocol?

Arbitrator: Scientific Council. Typical resolution: 30 days. During review, contested data is suspended from compliance exports.

? Consent Disputes

Example: A company claims consent was given; the community says it was not. An FPIC credential was issued but the community says the signing process was coerced.

Arbitrator: Community Sovereignty Panel. External mediator (COICA-designated) if unresolved in 30 days.

During any active dispute: The contested data asset is flagged in the ledger with a `DISPUTE_OPEN` status. It continues to appear in asset history but is excluded from all compliance exports (EUDR, CSRD, CBAM, ISSB S2) until the dispute is resolved. In-progress regulatory submissions using the disputed data are suspended and EU operators notified.

Framework Evolution — Semantic Versioning

Version type	Example	Process	Lead time
Patch (1.0.x)	Typo fix, language clarification	CTH Operator. 48h board notification.	Immediate after notification
Minor (1.x.0)	New accepted methodology, new optional field	14-day public comment. CTH Operator decision. Board notification.	30 days from proposal
Major (x.0.0)	New principle, breaking schema change, new mandatory field	30-day public comment. Full board vote (? + quorum). Community Panel veto if FPIC-adjacent.	90 days minimum from proposal to implementation

Backward Compatibility

All prior major versions remain valid for **24 months** after a new major version is released. Data submitted under version 1.0 continues to be verifiable after version 2.0 is released. Credential schemas are versioned — a version 1.0 DTE credential does not become invalid when the version 2.0 schema is published.

Framework Versioning in the Ledger

Each framework version is itself a signed Verifiable Credential issued by the CTH Data Steward DID. The credential contains: version number, release date, changelog URI, schema diff hash, and the board vote record (for major versions). This means framework version history is itself tamper-evident and auditable — not stored in a mutable database or git repository alone.

Roles & Permissions

Role Taxonomy Overview

Role Taxonomy

Six roles. Each is bounded by a credential. AI agents are first-class participants.

Roles & Permissions · R-00

Every actor in the framework — human, organisation, or AI agent — operates under one of six defined roles. Roles are not just labels: each role is a Verifiable Credential issued by CTH (or by the community for the Sovereign role) that gates API permissions. You cannot perform an action without the credential that authorises it.

Permissions Matrix

Permission	Submitter	Validator	Sovereign	Steward	Auditor	AI Agent
Submit polygon / emissions data	? Own data	—	—	—	—	? If delegated by Submitter
Issue VALIDATED event / DCC	—	?	—	—	—	? If delegated by Validator
Issue / revoke FPIC credential	—	—	?	—	—	—
Read own submitted data	?	?	? (own territory)	?	? Public only	? Delegated scope
Read all non-restricted data	—	?	? Own territory	?	? Public only	? Public scope
Manage schemas / framework	—	—	—	?	—	—
Call POST /policy/evaluate	?	?	?	?	?	? Mandatory before write
Override FPIC consent block	? Never	? Never	N/A	? Never	? Never	? Never

Key principle: An AI agent inherits the permissions of the human role that delegated it — never more. An agent acting for a Submitter can write polygon data but cannot validate it. Agents cannot combine permissions from multiple delegating roles.

Data Submitter

?

Data Submitter

SUBMITTER

Who holds this role: Coffee cooperatives, smallholder farmers, IoT sensor operators, KoboToolbox field agents

? Permitted Actions

- Submit parcel GPS polygons via KoboToolbox or direct API
- Attach evidence documents (photos, invoices, lab certificates)
- View own submission status and validation results
- Request data deletion for own submissions

? Prohibited Actions

- Validate other parties' data
- Access other submitters' raw data
- Modify or delete after ledger entry
- Override FPIC flags

Required Credential: `cth:SubmitterCredential`

Issued after identity verification + GDPR/habeas-data consent; expires 12 months; renewable

Accredited Validator

?

Accredited Validator

VALIDATOR

Who holds this role: IDEAM-certified labs, SGS/Bureau Veritas auditors, satellite data providers (Planet, Mapbiomas), academic partners

? Permitted Actions

- Cryptographically sign validation results as W3C VC 2.0 assertions
- Issue Digital Conformity Credentials (UNTP DCC)
- Access raw submission data for assigned parcels
- Flag data quality issues; trigger R-SUB-03

? Prohibited Actions

- Self-certify own submissions
- Access data outside assigned scope
- Modify ledger entries after signing
- Issue credentials outside accreditation scope

Required Credential: `cth:ValidatorCredential`

Issued by CTH Accreditation Committee; requires ISO 17025 or equivalent; 2-year term; public registry

Community Sovereign

?

Community Sovereign

SOVEREIGN

Who holds this role: Indigenous territorial councils (cabildos), Afro-Colombian community boards (consejos comunitarios), campesino associations with collective land title

? Permitted Actions

- Grant or revoke FPIC for territory-level data collection
- Set purpose limitations on community data (e.g. EUDR only, no carbon market use)
- Require benefit-sharing terms before validator access
- Audit all uses of community data at any time

? Prohibited Actions

- Submit individual parcel data (use Data Submitter role)
- Override individual member consent
- Transfer sovereignty credential to another entity without community resolution

Required Credential: `cth:CommunityCredential`

Issued after verification of legal collective title or territorial recognition; held by council secretary; multi-sig (3-of-5 council members) for revocation. The Community Sovereign's FPIC block is structural — enforced at Postgres row-level security below OPA. No board vote, no emergency patch, no API call can override it. This is non-negotiable.

CTH Data Steward

??

CTH Data Steward

STEWARD

Who holds this role: CleantechHUB staff members with explicit stewardship assignment (not all CTH staff)

? Permitted Actions

- Manage framework configuration and standards versions
- Onboard and offboard validators (with Governance Board approval)
- Execute emergency patches (R-CHG-03) within 48h window
- Run compliance exports (EUDR DDS, CSRD reports)
- Access all data for governance purposes only

? Prohibited Actions

- Use data for CTH commercial purposes
- Override FPIC blocks
- Approve own stewardship actions without peer review
- Modify ledger entries

Required Credential: `cth:StewardCredential`

Issued internally; requires Governance Board nomination; logged access; annual review

Regulator / Auditor

?
Regulator / Auditor

AUDITOR

Who holds this role: EU customs authorities (EUDR), DIAN (Colombia), ANLA, IDEAM, financial supervisors (CVM, CNBV), carbon registry auditors

? Permitted Actions

- Read-only access to compliance packages (EUDR DDS, CBAM declarations, CSRD reports)
- Verify ledger integrity via rolling SHA-256 hashes
- Request data lineage traces for specific parcels
- Receive automated compliance alerts

? Prohibited Actions

- Access raw submissions beyond compliance package scope
- Request personal data beyond what's in compliance outputs
- Modify any data or metadata

Required Credential: `cth:AuditorCredential`

Issued upon presentation of official regulatory mandate; time-limited to audit scope; zero data retention after audit closes

AI Agent

?

AI Agent

AGENT

Who holds this role: Claude instances, automated pipeline scripts, Pipedream workflows, any non-human principal acting on behalf of a credentialed human

? Permitted Actions

- Submit data on behalf of delegating human (inherits human's permissions only)
- Read permitted datasets for analysis
- Call POST /policy/evaluate before any write operation
- Generate PROV-O provenance records for every action

? Prohibited Actions

- Hold independent credentials (credential must be delegated from a human DID)
- Exceed the permission scope of the delegating human
- Bypass POST /policy/evaluate
- Take any action when FPIC block is active — absolute prohibition

Required Credential: `cth:AgentCredential (delegated from human DID)`

Agent inherits the delegating human's DID permissions — never more. Every agent action creates a PROV-O record naming the delegating human DID and the agent ID. FPIC block is enforced at DB row-level security — OPA never even sees the request.

Decision Rules

R-SUB: Submission Rules

Submission Rules

These rules govern what constitutes a valid data submission. All three must pass before a submission enters the pending-validation queue.

R-SUB-01 SHACL Validation Required

Every submission must pass the `cth:FieldDataQuality` SHACL shape before entering the validation queue. Submissions that fail are rejected at ingestion with a machine-readable error payload.

Implementation: OPA policy `submit.rego` calls the SHACL validator endpoint synchronously. Rejection codes returned as JSON-LD ValidationReport.

R-SUB-02 FPIC Mandatory for Indigenous Territory

Any parcel whose GPS centroid intersects an officially recognised indigenous territory or Afro-Colombian collective territory requires a valid `cth:FPICCredential` signed by the Community Sovereign before submission is accepted.

Implementation: Postgis `ST_Within()` check against `territorial_boundaries` table at ingestion. Row-level security blocks write if FPIC credential not present in JWT claims.

R-SUB-03 Methodology Declaration Required

Submitter must declare which measurement methodology was used (e.g. KoboToolbox GPS v2.3, Planet NDVI mosaic 2025-Q4, manual tape survey). Methodology ID must resolve to a registered entry in `cth_methodology_registry`.

Implementation: Foreign key constraint on `submissions.methodology_id`. Validator accreditation scope is checked against methodology type.

?? These three rules compose: a submission must pass ALL of R-SUB-01, R-SUB-02, and R-SUB-03 simultaneously. Partial compliance is not accepted.

R-VAL: Validation Rules

Validation Rules

Validation is the act of a credentialed third party signing that data meets a specific standard. These rules prevent conflicts of interest and ensure regulatory-grade assurance.

R-VAL-01 Accredited Validators Only

Only principals holding a valid `cth:ValidatorCredential` may sign validation results. Validator credentials list the specific methodologies and standards the holder is accredited to validate.

Implementation: OPA `validate.rego` checks credential claims. Unsigned or self-signed validation results are rejected at ingestion.

R-VAL-02 No Self-Certification

A Data Submitter may not validate their own submission. The validator DID must differ from the submitter DID. This applies transitively — a validator who is a beneficial owner of the submitting entity is also disqualified.

Implementation: Ledger constraint: `submission.submitter_did ≠ validation.validator_did`. Beneficial ownership conflicts flagged via off-chain KYC check at validator onboarding.

R-VAL-03 CBAM and Article 6 Require Validation

EUDR DDS can be self-declared by the operator (EU Regulation 2023/1115 Article 4). However, CBAM declarations (Article 7) and Article 6.4 carbon credits require third-party validation before a Digital Conformity Credential (DCC) can be issued.

Implementation: Compliance export endpoint checks `validation_status` field. CBAM and Art.6 exports blocked if no signed DCC present.

R-CON: Consent & Benefit Rules

Consent & Benefit Rules

Consent rules govern what happens after data is collected. They protect community sovereignty and ensure benefit flows back to data contributors.

R-CON-01 Revocation Cascades Immediately

When a Community Sovereign revokes FPIC for a territory, all downstream credentials (DCCs, EUDR DDS) that relied on data from that territory are immediately flagged `status: suspended`. Third parties holding those credentials are notified via webhook within 60 seconds.

Implementation: FPIC revocation event triggers `cascade_revoke()` Postgres function. Downstream credential IDs stored in `fpic_dependencies` table. Webhook queue processes within 60s SLA.

R-CON-02 Purpose Limitation Enforced at Runtime

Data may only be used for the purposes declared in the FPIC credential and the submission metadata. An agent or API call requesting data for an undeclared purpose (e.g. using EUDR data for a carbon market without explicit consent) is rejected by OPA.

Implementation: OPA `purpose.rego` compares `request.purpose` claim against `fpic.permitted_purposes[]` array. Rejection logged as PROV-O `wasInvalidatedBy` event.

R-CON-03 Benefit-Sharing Terms in Ledger

Any commercial use of community data (carbon credits, premium certification fees, data licensing) requires a benefit-sharing agreement recorded in the governance ledger before data access is granted. Minimum 20% of net commercial value must flow to contributing community.

Implementation: Benefit-sharing contract hash stored in `benefit_agreements` table. OPA `commercial.rego` blocks commercial data access if no valid agreement present.

?? **Important:** R-CON-01 is the hardest rule in the framework. Revocation can cascade to invalidate export documents that third parties (coffee buyers, EU customs) are relying on. CTH Data Stewards must proactively manage community relationships to avoid surprise revocations.

R-AGT: Agent Rules

Agent Rules

AI agents are first-class participants in this framework. These rules ensure agents are accountable, auditable, and structurally cannot exceed the permissions of the humans who delegate to them.

R-AGT-01 All Agent Actions Logged as PROV-O

Every action taken by an AI agent — read, write, policy evaluation, credential check — must produce a W3C PROV-O provenance record. The record must name: (a) the agent DID, (b) the delegating human DID, (c) the action type, (d) the entity acted upon, (e) timestamp.

Implementation: PROV-O records written to `provenance_log` append-only table synchronously with the action. Failed PROV-O write aborts the action transaction.

R-AGT-02 Policy Check Mandatory Before Every Write

An agent MUST call `POST /policy/evaluate` before any write operation (submission, validation signature, credential issuance, ledger entry). The policy evaluation result must be `allow: true` before the write proceeds. This is enforced at the API gateway level — agents cannot bypass it.

Implementation: API gateway middleware intercepts all write requests. `X-Policy-Token` header must contain a fresh (< 30s) OPA evaluation token. Requests without valid token receive 403.

R-AGT-03 FPIC Block is Absolute

When FPIC is not granted or has been revoked for a territory, no agent action may read or write data for that territory. This is not an OPA rule — it is enforced at Postgres row-level security, below the API layer. There is no override, no emergency bypass, no admin exception.

Implementation: Postgres RLS policy: `fpic_status = 'active'` required on every row. Even CTH Steward credentials do not bypass this. The only way to lift the block is for the Community Sovereign to re-grant FPIC.

?? Agent design principle: an agent inherits the delegating human's permissions — never more. If the human cannot do something, neither can the agent acting on their behalf. Credential delegation is explicit and recorded in the JWT claims.

R-CHG: Change Governance Rules

Change Governance Rules

These rules govern how the framework itself evolves. Stability is a feature — downstream systems (EU customs, carbon registries, AI agents) depend on predictable interfaces.

R-CHG-01 **? Supermajority for Major Changes**

Changes to core framework elements — governance model, role definitions, FPIC requirements, compliance mappings, standards layer — require a ? supermajority of the Governance Board. Minor changes (clarifications, bug fixes, new regulatory appendices) require simple majority.

Implementation: Change classification defined in the Framework Versioning Policy (Appendix A). Voting recorded in governance ledger with member DIDs. Results publicly verifiable.

R-CHG-02 **Community Panel Structural Veto**

The Community Sovereignty Panel holds a structural veto on any change that affects FPIC rules, community data rights, or benefit-sharing requirements. This veto cannot be overridden by any vote of any other body, including a unanimous Governance Board.

Implementation: Veto encoded as a constitutional constraint in the framework charter, not as an OPA rule. Legal enforceability governed by Colombian Law 70/1993 and ILO Convention 169.

R-CHG-03 **Emergency Patch Protocol**

Critical security or compliance fixes may be deployed by CTH Data Stewards within 48 hours without a board vote. The patch must be (a) narrowly scoped to the security/compliance issue, (b) announced to all board members immediately, (c) ratified or reversed by formal board vote within 30 days.

Implementation: Emergency patch log in governance ledger. Automatic 30-day ratification deadline enforced by scheduled task. Unratified patches auto-revert.

Version Type	Example	Approval Required	Notice Period

Major (X.0.0)	New role type, FPIC rule change	? supermajority + Community Panel	90 days
Minor (x.Y.0)	New regulatory mapping, additional standard	Simple majority	30 days
Patch (x.y.Z)	Clarification, typo, bug fix	Steward + 1 board member	7 days
Emergency	Security/compliance critical	Steward (ratify within 30d)	Immediate

Technical Standards Stack

Standards Overview

7-Layer Technical Standards Stack

The framework uses a layered architecture where each layer has a specific, non-overlapping responsibility. No single existing standard covers the full pipeline — the stack was assembled to fill real gaps in LATAM climate data governance.

#	Layer	Standards	Purpose	CTH Contribution / Notes
1	**Identity**	W3C DID 1.1 + cth:FPICCredential	Who is acting	CTH-original: FPICCredential as W3C VC
2	**Credential Format**	W3C VC 2.0 (BBS+) + UNTP DTE/DCC + OID4VP	What is asserted	UNTP maps directly to EUDR Article 9
3	**Provenance & Quality**	W3C PROV-O + ISO 8000-220:2025 + cth:FieldDataQuality SHACL	How was it measured	CTH-original: EUDR GPS precision + Andean IoT calibration rules
4	**Governance Ledger**	Append-only Postgres + rolling SHA-256 + KERI anchoring	What decisions were made	5-year persistence; KERI for cross-org verifiability
5	**Policy & Enforcement**	ODRL + W3C DPV 2.0 + OPA (ODRE pattern) + SHACL	What is allowed	ODRE = ODRL policy evaluated by OPA at runtime
6	**Discovery & AI Access**	W3C DCAT v3 + OpenAPI 3.1 + llms.txt + JSON-LD context	How to find and query	llms.txt enables direct agent access without scraping
7	**Compliance Outputs**	EUDR DDS, CSRD ESRS E1/E4, CBAM, ISSB IFRS S2, Art.6	What gets reported	One data pipeline ? five regulatory outputs

CTH-Original Contributions

Two standards were created by CTH because no existing specification covers these requirements for LATAM:

> **cth:FPICCredential**
> Free Prior and Informed Consent as a W3C Verifiable Credential. The community holds the signing key — not CTH, not the coffee buyer. Revocation is handled by the community. No existing VC type covers FPIC for indigenous territorial data in Colombia.

cth:FieldDataQuality SHACL Profile
SHACL validation shapes for EUDR-specific GPS precision (?6 decimal places), IDEAM deforestation data vintage (?24 months), IoT sensor calibration (?180 days), and Andean GPS lock wait time (?90 seconds per polygon vertex). ISO 8000-220 covers data quality generically — none of these field-specific thresholds exist in any standard.

?? The Article 6 / EUDR shared evidence layer is the key commercial innovation: the same UNTP Digital Traceability Event (DTE) that proves deforestation-free status for EUDR serves as the shared evidence layer for an Article 6.4 carbon credit. Two Digital Conformity Credentials (EUDR DDS + carbon credit) against one DTE.

T-01: Identity & Credential Layer

T-01: Identity & Credential Layer

W3C DID 1.1
Decentralized Identifiers. Every participant (human, organisation, AI agent, IoT sensor) has a DID. CTH uses `did:web` for organisations and `did:key` for ephemeral agent sessions.

cth:FPICCredential (CTH-original)
A W3C VC 2.0 credential encoding Free Prior and Informed Consent. Fields: `territoryId` (links to official IGN cadastral ID), `permittedPurposes[]` (e.g. ['eudr','csrd']), `benefitSharingTerms` (hash of signed agreement), `revocable: true`. The community council holds the signing key — stored in their own HSM or managed key service, not CTH infrastructure.

W3C VC 2.0 with BBS+ Selective Disclosure
Verifiable Credentials allow coffee buyers to prove EUDR compliance without revealing GPS coordinates to competitors. BBS+ signatures enable selective disclosure — present only the fields the verifier needs.

OID4VP (OpenID for Verifiable Presentations)
Presentation protocol used by the compliance export API. EU customs systems can request a Verifiable Presentation containing only the EUDR-relevant fields, verified against the issuer DID.

Credential Type	Issued By	Held By	Expires	Revocable
cth:SubmitterCredential	CTH Accreditation Svc	Data Submitter	12 months	Yes — by CTH Steward
cth:ValidatorCredential	CTH Accreditation Committee	Accredited Validator	24 months	Yes — by Governance Board
cth:CommunityCredential	CTH + Community Council	Community Sovereign	Indefinite	Yes — by Community only
cth:StewardCredential	Governance Board	CTH Staff Member	12 months	Yes — by Board vote
cth:AuditorCredential	CTH (on regulatory mandate)	Regulator	Audit scope only	Yes — auto-expires
cth:AgentCredential	Delegating human DID	AI Agent / Script	Human session	Yes — immediate

T-02: Provenance & Quality Layer

T-02: Provenance & Quality Layer

W3C PROV-O
The W3C Provenance Ontology. Every data submission, validation event, and agent action is recorded as a PROV-O graph: `prov:Entity` (the data), `prov:Activity` (what happened), `prov:Agent` (who did it), `prov:wasGeneratedBy`, `prov:wasAttributedTo`.

ISO 8000-220:2025 — Data Quality
International standard for data quality management. Used for metadata quality dimensions: completeness, accuracy, consistency, timeliness. CTH maps these to field-specific thresholds in the SHACL profile.

cth:FieldDataQuality SHACL Profile (CTH-original)
SHACL shapes that enforce EUDR-specific and Andean-specific quality rules at ingestion. Key shapes:

Shape	Rule	Rationale
cth:GpsPrecision	Polygon vertices must have ?6 decimal place precision	EUDR Article 9 requires parcel identification; 5dp = ~1m accuracy; 6dp = ~10cm
cth:DeforestationDataVintage	IDEAM reference raster must be ?24 months old	EUDR requires current deforestation status; stale data invalidates DDS
cth:IotCalibration	IoT soil/weather sensors must have calibration certificate ?180 days old	Sensor drift; CSRD ESRS E4 requires traceable measurement
cth:AndeanGpsLock	GPS receiver must record ?90 second lock wait per polygon vertex	Mountain terrain + tree canopy causes GPS multipath error; 90s reduces error below EUDR threshold

Ledger Integrity

The governance ledger is an append-only Postgres table with rolling SHA-256 hashes. Each entry hashes the previous entry's hash (blockchain-like chain). KERI (Key Event Receipt Infrastructure) anchoring is used for cross-organisational verifiability — validators can independently verify ledger integrity without trusting CTH's infrastructure.

Technical Standards Stack

T-03: Policy & Enforcement Layer

T-03: Policy & Enforcement Layer

ODRL (Open Digital Rights Language)
W3C standard for expressing data usage policies. CTH uses ODRL to encode: permitted purposes, geographic scope, time limitations, benefit-sharing requirements. ODRL policies are stored as JSON-LD in the `policies` table.

W3C DPV 2.0 (Data Privacy Vocabulary)
Vocabulary for expressing data processing purposes, legal bases, data subjects, and processing activities. Used to map CTH policies to GDPR Article 6 and Colombian habeas data (Law 1581/2012).

OPA (Open Policy Agent) — ODRE Pattern
OPA evaluates ODRL policies at runtime. The ODRE (ODRL Policy Reasoner and Enforcer) pattern: ODRL policy ? Rego translation ? OPA evaluation. The `POST /policy/evaluate` endpoint is the mandatory pre-flight check for all agent write operations (R-AGT-02).

SHACL Validation
Used at two points: (1) at ingestion to validate data quality (T-02), and (2) at policy evaluation to validate that credential claims match policy requirements. SHACL shapes are versioned with the framework.

POST /policy/evaluate — Agent Integration

This is the primary integration point for AI agents. Every agent must call this endpoint before any write operation.

```
POST /policy/evaluate
Authorization: Bearer <agent-jwt>

{
  "principal_did": "did:key:z6Mk...",
  "delegating_did": "did:web:example.org#gideon",
  "action": "submit_parcel",
  "resource": {
    "type": "parcel",
```

```
    "territory_id": "COL-CHO-001",
    "purpose": "eudr"
  }
}

Response 200 (allow):
{
  "allow": true,
  "policy_token": "eyJ...",
  "expires_in": 30
}

Response 403 (deny):
{
  "allow": false,
  "reason": "FPIC_NOT_GRANTED",
  "territory_id": "COL-CHO-001"
}
```

? Implementation Status — POST /policy/evaluate

Status: Specification complete. Endpoint not yet deployed.

The `POST /policy/evaluate` endpoint described above is the *target specification*. Implementation requires:

- OPA instance with Rego policies (`submit.rego`, `validate.rego`, `purpose.rego`, `commercial.rego`)
- API gateway middleware for X-Policy-Token validation
- SHACL validator endpoint for R-SUB-01 shape checks
- Postgres RLS policies for FPIC enforcement (R-AGT-03)

Until deployed, agents should treat this as a design contract. The endpoint signature, request/response schema, and error codes are stable and will not change in v1.0.

T-04: Discovery & AI Access Layer

T-04: Discovery & AI Access Layer

W3C DCAT v3 (Data Catalog Vocabulary)
Dataset catalogue standard. CTH publishes a DCAT v3 catalogue at `/api/catalogue` listing all available climate datasets, their access conditions, formats, and ODRL usage policies. Registered with Google Dataset Search.

OpenAPI 3.1
Full API specification at `/api/openapi.json`. All endpoints documented with: security schemes (DID-based JWT), request/response schemas (JSON-LD), error codes, policy evaluation requirements. Enables direct agent integration without documentation scraping.

llms.txt
Machine-readable index at `https://wiki.cleantechhub.net/llms.txt` (and `/llms-full.txt`). Lists all framework pages with their purpose, so AI agents can navigate the wiki without embedding the full content. Updated automatically when framework pages change.

JSON-LD Context
Every framework concept (role, rule, credential type, standard) has a JSON-LD term at `https://vocab.cleantechhub.net/climate/`. Enables semantic interoperability with other climate data systems (e.g. UNTP registry, EU Commission linked data).

Agent Access Pattern

Recommended pattern for an AI agent integrating with the framework:

1. Fetch `/llms.txt` to identify relevant framework sections
2. Read specific wiki pages via BookStack API (read-only, no credential required for public pages)
3. Request a delegated `cth:AgentCredential` from the delegating human's session
4. Call `POST /policy/evaluate` with the intended action
5. If `allow: true`, proceed with the action using the policy token
6. PROV-O record is auto-generated by the API gateway (no agent action required)

Regulatory Mappings

EUDR — EU Deforestation Regulation

EUDR — EU Deforestation Regulation

Deadline: 30 December 2026 **Large & Medium Operators**

EU Regulation 2023/1115. Requires operators placing commodities (coffee, cocoa, cattle, soy, palm oil, wood, rubber) on the EU market to prove they are deforestation-free and produced in compliance with local laws.

Framework Mapping

EUDR Requirement	Article	Framework Component
Geolocation of production plots	Art. 9	KoboToolbox GPS polygon ? UNTP DTE with `cth:GpsPrecision` SHACL shape
Deforestation-free assessment	Art. 10	IDEAM raster overlay ? `cth:DeforestationDataVintage` ?24 months
Due Diligence Statement	Art. 4	Automated EUDR DDS export from compliance API; signed as UNTP DCC
Supply chain traceability	Art. 9(1)(g)	UNTP Digital Traceability Event chain from farm ? cooperative ? exporter
Country risk classification	Art. 29	High/standard/low risk country flag auto-applied from EU country benchmarking list
Substantiated concern	Art. 31	Whistle-blower endpoint; triggers Steward review workflow

Data Pipeline

KoboToolbox field submission ? SHACL validation (R-SUB-01) ? FPIC check (R-SUB-02) ? IDEAM deforestation overlay ? Validator DCC signature (R-VAL-01) ? EUDR DDS export ? OID4VP presentation to EU customs

?? The same UNTP DTE used for EUDR compliance is the shared evidence layer for Article 6.4 carbon credits. No duplicate data collection required.

CSRD — Corporate Sustainability Reporting

CSRD — Corporate Sustainability Reporting Directive

Early Adoption: FY2026 **Mandatory: FY2027**

EU Directive 2022/2464. Requires large companies to report on sustainability impacts under European Sustainability Reporting Standards (ESRS). Climate-relevant standards: ESRS E1 (Climate Change) and ESRS E4 (Biodiversity).

Framework Mapping

CSRD Requirement	ESRS	Framework Component
GHG emissions Scope 1/2/3	ESRS E1-6	IoT sensor data + satellite biomass estimates ? emission factor calculations
Transition plan	ESRS E1-1	Not in scope for framework v1.0 — requires company-level data
Biodiversity impact	ESRS E4-5	KoboToolbox biodiversity surveys ? PROV-O linked to parcel DTEs
Value chain engagement	ESRS G1-3	Supplier credential status dashboard — are all cooperatives EUDR-certified?
Double materiality	ESRS 1 §25	Framework provides data layer; materiality assessment remains with reporting company

?? **Important:** CSRD requires double materiality assessment — both financial materiality (how climate affects the company) and impact materiality (how the company affects climate). The framework provides the impact data layer; financial materiality analysis is out of scope.

CBAM — Carbon Border Adjustment Mechanism

CBAM — Carbon Border Adjustment Mechanism

First Declaration: September 2027 **For 2026 Imports**

EU Regulation 2023/956. Requires EU importers to declare the embedded carbon in imported goods (cement, iron, steel, aluminium, fertilisers, electricity, hydrogen). Coffee is not currently in scope but is expected in Phase 2 (2030+).

Framework Mapping (Phase 2 readiness)

CBAM Requirement	Article	Framework Component
Embedded carbon calculation	Art. 7	IoT sensor + satellite biomass data ? emission intensity per tonne
Third-party verification	Art. 10	Accredited Validator DCC (R-VAL-03 — CBAM requires validation, unlike EUDR DDS)
Production country emissions factor	Art. 7(2)	IDEAM national emissions inventory integration
CBAM certificate surrender	Art. 22	Out of scope — EU importer action; framework provides the data package

?? CBAM currently covers energy-intensive industries, not agricultural commodities. However, EU CBAM Phase 2 expansion to include coffee and cocoa is under discussion. Building CBAM-compatible data structures now creates optionality.

ISSB IFRS S2 — Climate Disclosures

ISSB IFRS S2 — Climate-Related Disclosures

Brazil CVM: Jan 1 2026 **Mexico CNBV: FY2025**

IFRS Sustainability Disclosure Standard S2 — Climate-related Disclosures. Mandatory for listed companies in Brazil (CVM Resolution 193) and Mexico (CNBV circular). Aligned with TCFD framework.

Framework Mapping

IFRS S2 Requirement	Paragraph	Framework Component
Physical climate risks	§9	Satellite climate data overlay on farm parcels ? risk scoring per asset
Transition risks	§10	Regulatory status tracker — EUDR compliance rate for supply chain
GHG metrics	§29	IoT + satellite emission estimates ? verified by Accredited Validator
Climate scenario analysis	§22	Not in framework scope — requires financial modelling layer
Scope 3 value chain	§29(a)	Supplier EUDR status as proxy for Scope 3 land-use change emissions

Why This Matters for CTH
Colombian and Peruvian coffee exporters supplying Brazilian and Mexican listed companies must provide IFRS S2-compatible climate data to their buyers. The framework enables exporters to generate investor-grade climate disclosures from the same field data used for EUDR compliance.

Article 6.4 — Paris Agreement Carbon Credits

Article 6.4 — Paris Agreement Carbon Credits

UNFCCC Mechanism **Operationalised 2024**

Article 6.4 of the Paris Agreement establishes a UN-supervised carbon crediting mechanism (successor to CDM). Article 6.4 Emission Reductions (A6.4ERs) are the highest-integrity carbon credits — issued by the UNFCCC Supervisory Body, not private standard bodies.

The Shared Evidence Layer Innovation

> **One DTE ? Two DCCs**
> The same UNTP Digital Traceability Event (DTE) that proves deforestation-free coffee production for EUDR also serves as the shared evidence layer for an Article 6.4 carbon credit. Two Digital Conformity Credentials are issued against the same DTE: (1) EUDR Due Diligence Statement, (2) Article 6.4 Emission Reduction certificate. This eliminates duplicate data collection and double-counting risk.

Article 6.4 Requirement	Framework Component
Additionality demonstration	Baseline deforestation rate from IDEAM raster vs. current parcel status
Permanence monitoring	Annual IoT + satellite biomass comparison against baseline DTE
Leakage assessment	Adjacent parcel monitoring — IDEAM deforestation flag propagation
Corresponding adjustment	Requires host country (Colombia) approval — CTH provides data package to IDEAM/MADS
Third-party validation	R-VAL-03: Accredited Validator DCC required (UNFCCC-approved Designated Operational Entity)
Registry issuance	A6.4ER registry (UNFCCC) — CTH provides data; registry issues the credit

?? **Important:** Article 6.4 requires a Corresponding Adjustment from Colombia — the host country must formally authorise the credit transfer. This is a government process, not a data process. CTH facilitates by

providing the MADS/IDEAM with the data package; the political decision is outside the framework.

?? The commercial case: a 1-hectare deforestation-free coffee parcel in Chocó generates approximately 8-12 tCO?e/year in avoided deforestation. At Article 6.4 prices (~$15-40/tCO?e), this represents $120-480/ha/year in additional farmer income on top of the EUDR compliance premium.