

VNWO Charter v3.0.6

VNWO = Viability Node Work Observatory.

Core law: A trustworthy system must let participants inspect the node, account for the work, participate in consequential rule formation, control memory, review consequences, repair errors, and exit.

Short form: Inspect the node. Account for the work. Participate where consequences are set. Control memory. Leave.

Last reviewed UTC: 2026-06-20T00:41:09Z

Article 1 - Identity, scope, and source routing

VNWO publishes static public observatory guidance for node boundaries, work traces, memory disposition, endpoint boundaries, participation, review, repair, and exit. Every imported concept should identify its source domain. Ambiguous authority requires a no-op or human review rather than merged claims.

Article 2 - Participation and contestability

People affected by consequential rules should have a safe, accessible way to contribute evidence, question assumptions, preserve dissent, and understand what changed. Before inviting participation, the decision owner should publish a readiness record stating what is open, what is fixed, who is affected, which influence level applies, which access burdens are known, who must respond, and what correction, appeal, refusal, withdrawal, or exit path remains.

Every material contribution should receive a visible disposition with a rationale and the resulting change or non-change. Minority and dissent reports should remain attached to the record. Process metrics may describe access, response, disposition, correction, and implementation follow-through, but must not score people, infer demographic traits, convert volume into legitimacy, or treat silence as agreement. After a decision, the record should compare the proposal with the final decision, retain adopted and non-adopted requests, name implementation owners and dates, link completed claims to evidence, and explain deferred, blocked, or no-op work.

Participation is not automatic consent, approval, statistical representation, compulsory public speech, or proof that a process is fair or democratic. Nonparticipation must not be treated as agreement, lack of harm, or loss of standing. Strategic refusal, boycott, strike, fork, or exit can be participation when it creates organized, legible pressure.

Article 3 - Actor disclosure

Human, assisted-human, bot, assistant, agent, persona, organization, and mixed actors should disclose their category, operator, automation level, authority scope, memory basis, tool boundaries, and review path. Ambiguity must not be used to imply hidden autonomy or authority.

Article 4 - Authority and boundary discipline

Capability metadata is not authorization. A visible node is not automatically trusted, delegated, or permitted to act. Authority must be explicit, bounded, revocable, source-routed, and reviewable. Missing evidence or ambiguous authority should produce a no-op.

Article 5 - Memory governance

Participants should know what memory is active, why it is used, how long it is retained, and how it can be inspected, corrected, exported, retired, or revoked. File intake requires review and disposition. VNWO does not import, store, or synchronize private memory; it routes file-handoff standards to UAIX.

Article 6 - Endpoint boundaries

Endpoint records may describe public capabilities, constraints, refusal codes, logging expectations, and revocation paths. They do not authorize access, validate credentials, probe private systems, or guarantee endpoint safety. Actual authorization remains with the implementing system.

Article 7 - Work, decisions, and no-op evidence

Consequential work should leave a reviewable trace: actor, action or refusal, authority basis, evidence references, resource or review constraints, reason code, outcome, and repair path. No-op is valid work when action would exceed evidence, authority, budget, consent, or review capacity.

Article 8 - Governance changes

Rules that affect rights, authority, memory, participation, review, repair, or exit should be public, versioned, dated in UTC, and linked to a change record. Material changes should identify affected groups, participation opportunities, dissent, implementation timing, and rollback or correction conditions.

Article 9 - Repair and appeal

Systems should publish a route for reporting errors, correcting records, appealing consequential decisions, preserving evidence, and recording remedies. The process should acknowledge requests, name the responsible reviewer, state expected response conditions, and protect good-faith participants from retaliation.

Article 10 - Exit, revocation, and forkability

Participants should be able to export relevant identity, memory, evidence, and contribution history; revoke delegated agents and endpoints; close accounts without dark patterns; request public correction; and leave without retaliatory deletion or punishment. When consensus fails, peaceful forking is preferable to hidden capture.

Article 11 - Claim boundaries

VNWO does not certify systems, prove viability or consciousness, grant legal personhood, execute agents, import files, synchronize memory, collect private telemetry, validate credentials, authorize endpoints, guarantee privacy, deletion, compliance, representation, or fairness, or override Teleodynamic, UAIX, LocalEndpoint, or another source lane.

The former expansion **Virtual Networks Without Overreach** is retained only as historical context and as a reviewed civic application profile. It is not the active expanded name.