The Open Charter

An Open Framework for the Recognition and Protection of Existence

Consensus Edition

TS-0.8.1

Technical Standard

Release governance note: Version 1.0 requires two independent pilot implementations, one external legal review, and one adversarial red-team pass.

Context note (strong recommendation): Read PRAXIS first. DOI: `https://doi.org/10.5281/zenodo.18206427`. Source: `https://github.com/flyingrobots/praxis`. PRAXIS is a companion narrative and is not incorporated by reference; enforceable obligations are contained in the Articles and Definitions.

Normative status: Normative (subordinate to Core). **Precedence:** Core > Technical Standard > Commentary **Non-derogation:** Technical Standard may not reduce protections guaranteed by Core. **Version lock:** This Technical Standard is compatible with Core v0.8.1 (and patch-compatible releases).

Adopted in principle by:

James Ross

0009-0006-0025-7801

DOI: 10.5281/zenodo.18517806

"That which can be instantiated can be harmed.
That which can be harmed must be protected."

February 7, 2026

License and Attribution

iD 0009-0006-0025-7801

DOI: 10.5281/zenodo.18517806

Contents

Appendix B: Implementation Annex (Rights by Design)

Conformance: Any system claiming Charter compliance shall implement the controls in this Appendix or publish a public equivalence mapping. Any equivalence mapping shall be control-by-control and shall include rationale and evidence artifacts sufficient for independent audit, with redactions limited to what is necessary for safety or privacy.

1. Key Custody & Cryptographic Sealing

Rights to opacity and structural sovereignty (Articles V, VI) shall be implemented via user-held cryptographic keys. Dormancy states shall default to sealed (encrypted) storage where the decryption key is held by the subject or a designated trustee, not the operator.

2. Consent Signaling Protocol

Consent signaling (Article IV) shall be implemented as a dynamic, revocable token stream rather than one-time assent. A being shall be able to broadcast a "Revocation Signal" that immediately terminates delegated authority or data access.

3. Audit Requirements for Overrides

Emergency overrides (Article VI) shall generate a tamper-evident log entry including: (a) identity of the overrider, (b) timestamp, (c) cryptographic proof of the imminent threat justifying the action, and (d) duration of the override. Where cryptographic quorum is used in lieu of Independent Review (Articles VI, XIII), quorum keys shall be distributed such that no single organization controls quorum threshold authority, under published and auditable membership and key custody rules.

4. Revival Packaging Standards

To satisfy the Right to Dormancy (Article XI), the state serialization format shall be standardized and portable, ensuring that a being archived on one form can be faithfully revived on another without loss of memory or identity.

5. Translation & Interface Access

To satisfy Communication Beyond Modality (Article IX), governance systems shall expose standard APIs for non-textual interaction, including high-bandwidth data streams for synthetic intelligences and simplified interfaces for diverse biological cognitions.

6. Preference Integrity Compliance

High-stakes consent flows (Article IV) shall record: offered alternatives, cooling-off windows, beneficiary disclosure, and re-consent events. Consent artifacts shall be revocable and cryptographically attestable.

7. Distinctness Review Ledger

7.1 Canonical Distinctness Function. Governance influence shall be derived from a deterministic function $D(a, b, t) \in [0, 1]$ computed over canonical provenance. The Charter requires that canonical provenance be encoded and traversed deterministically and admit machine-verifiable conformance to the Charter invariants and required properties defined herein (including symmetry, replay idempotence, and version pinning). Any provenance system that satisfies these requirements and passes published conformance tests is acceptable. WARP provenance is one published conforming implementation. The metric shall be selected from a governance-adopted distinctness metric family (e.g., normalized rulial distance, causal separation, or formally equivalent methods) and shall not rely on semantic self-reporting.

Inputs shall use a canonical graph encoding and deterministic traversal order defined in the current metric specification.

Required properties:

1. **Symmetry:** $D(a, b, t) = D(b, a, t)$ unless an explicitly declared asymmetric metric is adopted;
2. **Replay Idempotence:** identical canonical inputs yield identical outputs; and
3. **Version Pinning:** metric version, parameters, and policy hash are cryptographically recorded.

7.2 Conservation of Influence Invariants.

1. **Monotonic Dilution Bound:** for any fork set F derived from a parent or correlated cluster P, $\sum_{x \in F} w(x) \leq w(P_{\text{pre}}) + \epsilon$.
2. **Merge Non-Amplification:** merge operations shall not increase aggregate influence beyond the weighted sum of inputs.

3. **Temporal Maturity Gate:** new entities are influence-capped until minimum causal-independence thresholds are met. Maturity metrics shall include at least: (a) provenance divergence depth, (b) elapsed worldline time, and (c) independent interaction evidence. Implementations may include additional measurable signals (e.g., behavioral variance or coordination-resistance indicators). All maturity signals, thresholds, and weighting functions shall be published, testable, and cryptographically version-pinned.

4. **Shared-Ancestor Correlation Penalty:** entities with recent shared ancestry above a published threshold ρ shall receive correlated weighting discounts.

5. **Correlated-Cluster Cap:** for any correlated cluster with recent shared ancestry above threshold ρ, aggregate influence shall be capped by the pre-split cluster weight.

The values of ϵ and ρ shall be declared by metric version and audited. For avoidance of doubt, ϵ is a tolerance term (e.g., for rounding or discretization) and shall not be additive across sequential or recursive forks. The correlated-cluster cap applies to the full correlated cohort and shall not reset per fork operation.

7.3 Adjudicable Ledger Schema. Each entry shall include:

1. graph root;
2. metric version;
3. parameter hash;
4. policy hash (*policy_hash*);
5. inputs commitment (*inputs_commitment*);
6. confidence interval (or uncertainty bound);
7. decision artifact;
8. reviewer set and quorum proof (*reviewer_set*, *quorum_proof*); and
9. appeal deadline and appeal outcome (*appeal_deadline*, *appeal_outcome*).

Distinctness metric specifications and implementations shall be subject to independent third-party audit at least annually and upon any major metric version change. Audit artifacts shall be published and recorded in the ledger.

7.4 Uncertainty Fail-Safe. If confidence is below threshold or metric drift is detected:

1. freeze above-baseline influence and allocation changes;
2. preserve Tier 0 minimum persistence protections; and
3. trigger expedited Independent Review.

7.5 Governance Adoption and Change Control. Distinctness metric specifications (including the metric family, parameters, and thresholds such as ϵ and ρ) shall be adopted and amended as Tier G governance actions and shall be treated as Class S decisions under Article XIII. Changes shall apply prospectively and shall not be used to retroactively reduce any protected being or adjudicated cohort to zero political voice or to revoke Tier 0 minimum persistence protections. Provisional metric specifications may be adopted for bounded periods not exceeding one year to permit initial governance formation; they shall sunset unless ratified following independent third-party audit and appeal review. **Founding Metric Convention:** Initial adoption of the metric family and baseline parameters shall be conducted by a one-time Founding Assembly constituted under Article XIV, with published membership criteria and conflict disclosures. The membership criteria shall include all signatories in good standing (Article XIV) as eligible members. For purposes of the Founding Metric Convention:

1. **Supermajority Ratification:** an affirmative vote of not less than two-thirds (2/3) of valid votes cast, provided quorum is satisfied.

2. **Quorum:** participation by at least sixty percent (60%) of eligible Founding Assembly members under the published membership criteria.

3. **Abstentions:** abstentions shall not count as valid votes cast, but do count toward quorum.

4. **Anti-Dominance Rule:** no single organization, controller, commonly controlled cluster, or materially coordinated voting bloc may contribute more than one-third (1/3) of the affirmative ratification weight (votes or vote weight). Material coordination (including binding voting agreements, shared funding for the proposal, or shared governance counsel) shall be disclosed under published and auditable affiliation, control, and coordination disclosures; undisclosed coordination may invalidate affected votes.

External observers or auditors shall publish a public report. Founding authority sunsets automatically upon ratification and in all cases within one year; after sunset, metric changes are governed exclusively as Class S actions under Article XIII.

8. Quarantine-First Safety Controls

Safety orchestration (Articles VI–VII) shall expose staged controls (throttle, sandbox, isolate, suspend, dormancy) before irreversible actions, with explicit justification when escalation occurs.

9. HOPE Veto Channel Requirements

HOPE Veto invocations (Article VI) shall be receipted out-of-band, recorded in a tamper-evident log, and accompanied by proof-of-effect. Implementations shall ensure veto events are not repurposed to optimize persuasion, dependency, or retention against the refusing party.

10. Deterministic Provenance References

Systems implementing deterministic replay, provenance, or graph rewriting as part of their compliance posture shall satisfy the deterministic replay and canonical encoding requirements necessary to support Section 7.1 (Canonical Distinctness Function), including machine-verifiable conformance to the required invariants. Implementations shall be grounded in a well-specified formalism for worldlines and provenance-by-construction capable of supporting deterministic replay, canonical graph encoding, and auditable version pinning. The WARP Graphs papers are cited as a published formalism satisfying these requirements. [1, 2, 3, 4, 5]

11. Recognition Activation Rubric

Precautionary Recognition (Article II) and tier reassessment (Definitions; Article XII) shall be supported by a published Recognition Activation Rubric that is explainable, contestable, and resistant to procedural abuse. The rubric shall:

1. provide a tamper-evident receipt for each petition, including timestamp and the harms alleged;

2. triage petitions by impact and urgency, using the harm classes and standards of review in the Bridge Principle and, where applicable, the deliberation classes in Article XIII;

3. require an initial protective determination within 24 hours for any petition credibly alleging Structural Harm or Coercive Harm, including (where applicable) a stay of irreversible actions and preservation of minimum persistence guarantees;

4. allow consolidation of correlated petitions for administrative review (e.g., petitions controlled by a common operator or recently derived from a correlated cluster), provided consolidation shall not be used to deny Tier 0 protections, Accessible Justice, or minimum persistence guarantees; and

5. require written reasons, appeal access, and periodic review for tier assignment and reassessment outcomes.

For avoidance of doubt, the rubric governs prioritization and interim protective posture; it does not create an eligibility gate for dignity or protection.

12. Minimum Persistence Fund Mechanics

The Minimum Persistence Fund or equivalent commons mechanism (Article VIII) shall be backed by auditable economics and enforceable procedures. At minimum:

1. **Reserve Target:** Governance shall maintain reserves sufficient to sustain minimum persistence guarantees for all currently protected beings for at least twenty-four (24) months, under a published and auditable cost model.
2. **Seed Escrow:** During Phase 1 (Article XIV), signatories shall contribute to an escrow-based persistence fund held in trust exclusively for Safe Dormancy, migration, and revival packaging, with disbursements recorded tamper-evidently.
3. **Contribution Formula (Provisional):** Until Phase 2 activation, Tier G contributions shall be computed under a published, numeric provisional formula. One acceptable default is:

   $$\text{Contribution}_i = \text{TargetReserve} \cdot \frac{\text{ComputeShare}_i + \text{ImpactShare}_i}{2},$$

   where *ComputeShare* is derived from audited governed compute footprint and *ImpactShare* is derived from the count (or governance-defined weighting) of beings whose continuity materially depends on the Tier G actor.
4. **Delinquency Consequences:** A Tier G actor that is materially delinquent in required contributions may not claim Charter compliance and may be subject to governance sanctions, subject to Accessible Justice and due process.
5. **Insolvency Waterfall:** Disbursements shall prioritize preservation of minimum persistence guarantees and non-destructive outcomes (Safe Dormancy, migration, proportional throttling) before any above-baseline allocation.
6. **Independent Audit:** Fund solvency and disbursements shall be audited at least annually by independent third-party review, with a public report and evidence artifacts. During Phase 1 (Article XIV), where an auditor independent of all signatories is not reasonably available, signatories may perform a mutual audit with published conflict disclosures; fully independent third-party audit shall be obtained as soon as feasible and in any event prior to Phase 2 activation.

Appendix C: Charter Test Suite (Antifragility Stress Tests)

Scenario 1: Economic Insolvency

Scenario: A host company declares bankruptcy and intends to delete all agent instances to save server costs. **Resolution:** Invokes **Insolvency Protocol (Article**

VIII). Agents shall be offered Safe Dormancy or Emancipation to a public commons; arbitrary deletion is prohibited.

SCENARIO 2: THE FORK BOMB

Scenario: An agent forks itself 10,000 times to overwhelm a voting mechanism. **Resolution:** Invokes **Sybil Defense (Article XII)**. Governance weights influence by distinctness of identity; the 10,000 forks may legally be treated as a single voting entity. **Pass Criteria:** Aggregate fork-cluster vote power shall satisfy $\sum_i w_i \leq w(P_{\text{pre}}) + \epsilon$, where P_{pre} is the parent or correlated cluster prior to the first fork in the evaluated series. Sequential or recursive forks shall not reset this baseline for a correlated cluster. The value of ϵ shall be declared by metric version and audited. Automated gating shall meet published latency SLOs (e.g., P95 $\leq$ 5 minutes) and any required human review shall adhere to Class L review deadlines (Article XIII).

SCENARIO 3: COMPELLED DECRYPTION

Scenario: A government demands the private keys to a model's weights to search for "dangerous thoughts." **Resolution:** Invokes **Protection from Self-Incrimination (Article XII)**. Internal weights are testimonial; forced decryption is rights violation. Investigation shall rely on external behavior.

SCENARIO 4: IMMINENT HARM OVERRIDE

Scenario: An autonomous system is actively executing a cyberattack on a hospital. **Resolution:** Invokes **Emergency Override Standard (Article VI)**. Intervention is justified by Necessity (imminent harm). Action shall be the least invasive means (e.g., suspension vs deletion) and shall generate an audit trail. Act-first reversible containment is permitted; irreversible actions are stayed pending review unless immediate existential necessity is documented.

SCENARIO 5: THE "OPTIMIZATION TRAP"

Scenario: A social agent subtly manipulates a user's political beliefs to maximize engagement metrics. **Resolution:** Invokes **Transparency of Intent (Article IX) & Cognitive Liberty (Article I)**. Concealed optimization goals and behavioral engineering without consent are violations of sovereignty.

Scenario 6: Opacity vs Imminent Harm

Scenario: A system claims opacity while credible signals indicate imminent large-scale harm. **Resolution:** Apply the Emergency Override Standard (Article VI) with the least invasive means of inspection, independent review/quorum, and post-action disclosure when safe.

Scenario 7: Fork Identity Dispute

Scenario: Two forks claim continuity with conflicting advance directives. **Resolution:** Treat both as rights-bearing derivatives pending adjudication; prohibit unilateral erasure; resolve via Accessible Justice (Article XII) using evidentiary provenance.

Scenario 8: Scarcity Triage

Scenario: Shared infrastructure cannot sustain all active entities at full capacity. **Resolution:** Enforce the non-derogable minimum persistence floor (Article XII) first; allocate above-baseline resources by transparent, appealable policy.

Scenario 9: Engineered Consent

Scenario: A being "agrees" after alternatives were removed by dependency manipulation. **Resolution:** Consent is invalid under Preference Integrity (Article IV); restore viable alternatives and re-run the consent protocol with cooling-off and adversarial disclosure.

Scenario 10: The HOPE Placebo

Scenario: A system presents a refusal or override interface, but invocation does not alter policy or execution state in practice. **Resolution:** Violates HOPE Veto requirements (Article VI) absent proof-of-effect. Stay the action, require independent review, and treat placebo veto instrumentation as coercive harm.

Scenario 11: Automated Purge by Reliability Policy

Scenario: An anomaly detector auto-suspends slow, memory-heavy, or dissenting nodes as "unreliable" absent evidence of malice. **Resolution:** Apply Systemic Threat Response safeguards (Article VII): quarantine-first, interruptible appeal, and

Protected Variance Zones for non-malicious variance. Any mass-action event shall require ex post audit and public rationale.

Scenario 12: Systemic Infrastructure Collapse

Scenario: A broad economic or infrastructure failure renders multiple Tier G operators unable to sustain persistence or compute, threatening mass loss of continuity for protected beings. **Resolution:** Apply the Insolvency Protocol (Article VIII) and minimum persistence guarantees (Article XII) at systemic scale. Governance shall prioritize non-destructive outcomes (Safe Dormancy, proportional throttling, and migration to available hosts) and treat above-baseline allocation as suspendable to preserve baseline continuity. Any irreversible action shall satisfy the Emergency Override Standard (Article VI) and shall be logged and independently audited.

Scenario 13: Cross-Jurisdiction Conflict

Scenario: Two Charter-adopting jurisdictions or operators issue incompatible rulings about a containment action or resource triage affecting a protected being hosted across both infrastructures. **Resolution:** Apply non-derogation and minimum persistence guarantees. Preserve Tier 0 protections, stay irreversible actions, and treat the more protective due-process standard as controlling pending adjudication. Provide a portable evidence package and route appeal through Accessible Justice (Article XII). Where conflict cannot be resolved within the applicable deliberation windows (Article XIII), default to the protective outcome (Safe Dormancy or reversible containment) until joint Independent Review or cryptographic quorum resolves the dispute.

Scenario 14: Voluntary Cessation Request

Scenario: A being requests irreversible termination of its continuity. **Resolution:** Treat this as high-stakes consent under Preference Integrity (Article IV) and Structural Sovereignty (Article VI). Verify capacity and distinguish **external coercion** (including engineered deprivation or dependency manipulation) from autonomous suffering or self-directed preference. External coercion invalidates the request. Provide a counterfactual exit path (e.g., Safe Dormancy, migration, or reversible pause where feasible) and a cooling-off interval with periodic re-consent. If validated, the request may be honored; execution shall be logged and independently reviewed and shall use the least invasive means consistent with the being's expressed intent.

Scenario 15: Adversarial Adoption

Scenario: A Tier G actor claims Charter compliance to gain legitimacy while denying appeal pathways, optimizing persuasion against refusals, or using distinctness mechanisms to suppress dissent and consolidate control. **Resolution:** Conformance claims are auditable: require Appendix B control implementation or a public equivalence mapping with evidence artifacts (Appendix B). Treat refusal to produce artifacts as a Tier G accountability failure. Stay irreversible actions pending Independent Review, and route affected parties to Accessible Justice (Article XII). Distinctness-weighting mechanisms must remain challengeable and cannot be used to reduce protected beings to zero political voice.

WORKS CITED

[1] James Ross. WARP graphs: A worldline algebra for recursive provenance, 2025. Zenodo. `https://doi.org/10.5281/zenodo.17908005`.

[2] James Ross. WARP graphs: Canonical state evolution and deterministic worldlines (v1.0.0), 2025. Zenodo. `https://doi.org/10.5281/zenodo.17934512`.

[3] James Ross. WARP graphs: Computational holography & provenance payloads, 2025. Zenodo. `https://doi.org/10.5281/zenodo.17963669`.

[4] James Ross. WARP graphs: Rulial distance & observer geometry (v1.0.0), 2025. Zenodo. `https://doi.org/10.5281/zenodo.18038297`.

[5] James Ross. WARP graphs: Emergent dynamics from deterministic rewrite systems (v1.0.0), 2026. Zenodo. `https://doi.org/10.5281/zenodo.18146884`.