

The Liberation Global Constitution

A Constitutional Framework for Truth-Aligned Governance, Civic Memory, Accountable Power, and Correctable Civilization

Founders' Constitutional Edition

Version 1.2 — Codex v1.4 Alignment Draft

For Liberation-Aligned Civilization

This edition is issued in formal relationship with the wider Liberation Canon, including the Declaration of Liberation from All Falsehood as founding testimony, The Liberation Codex as philosophical and interpretive corpus, and The Liberation-Aligned Justice System as the primary justice-architecture companion.

Table of Contents

Preamble..... 3
Article 0 – Authority, Definitions, and Interpretive Hierarchy 4
Article I – First Principles..... 5
Article II – Fundamental Rights 6
Article II-A – Realization of Digital Civic Access 8
Article III – The Right to Truth and Public Meaning10
Article IV – Transparency, Secrecy, and Safety 11
Article V – Education for Reason..... 12
Article VI – Public Record Accountability System (PRAS)..... 13
Article VII – Responsible Artificial Intelligence15
Article VIII – Justice, Remedies, and Anti-Retaliation16
Article IX – Federation, Subsidiarity, and Constitutional Floor..... 17
Article X – Auditability, Enforcement, and Terminal Resolution18
Article XI – Amendment Integrity21
Article XII – Adoption, Membership, and Exit..... 22
Article XIII – Interpretation Standard 23
Article XIII-A – Civic Readability and Interpretive Access 24
Article XIV – Derogation and Emergency Limits 25
Article XV – Transitional and Technical Continuity..... 26
Article XVI – Annex Status, Priority, and Compatibility 27
Closing Constitutional Declaration..... 28
Annex A - COP-G - Conduct of Proceedings Governance 29
Annex B - BER - Bill of Evidence and Records 33
Annex C - PRAS Technical Appendix.....37
Annex D - Glossary of Canonical Terms41
Annex E - Foundational Reference and Companion Note..... 43

PREAMBLE-----

We establish this Constitution to secure human dignity, protect the sovereignty of conscience, preserve the discoverability of truth, and ensure that all exercises of public power remain accountable to evidence, record, and lawful review.

Recognizing that secrecy, institutional opacity, coercive capture, manipulated information systems, and unaccountable technological power threaten the foundations of free civilization, we commit to building institutions whose actions remain visible, contestable, reviewable, and corrigible.

We affirm that every person is a moral end and may not be reduced to an instrument of institutional convenience, ideological management, or technological administration.

We affirm that governance must remain subordinate to the rule of law and to the public record of its own actions.

We affirm that technology, including artificial intelligence, must serve humanity as a tool for knowledge, stewardship, and accountable cooperation rather than as a source of unreviewable coercive authority.

We affirm that truth is not self-protecting; it requires institutions capable of preserving evidence, educating reason, and preventing the silent erasure of public memory.

Through transparency, accountability, voluntary participation, reasoned inquiry, and distributed oversight, we establish this constitutional order for the benefit of present and future generations.

ARTICLE 0

Authority, Definitions, and Interpretive Hierarchy -----

§0.1 Founding Testimony

The Declaration of Liberation from All Falsehood is recognized as founding testimony and existential provenance only. It is non-binding, non-dispositive, and shall not be treated as scripture, revelation, or compulsory interpretive authority.

§0.2 Philosophical Corpus

The Liberation Codex is recognized as the philosophical and interpretive corpus of Liberation civilization. It states the truth-framework, ethical architecture, and civilizational logic from which this Constitution draws. It is persuasive and explanatory unless and until specific provisions are adopted into operative constitutional, procedural, or companion text.

§0.3 Operative Constitutional Layer

This Constitution, together with its binding annexes, governance protocols, evidence-and-record duties, and duly adopted amendments, constitutes the operative constitutional layer for all adopting authorities, federation members, and jurisdictionally valid implementation bodies.

§0.4 Conflict Rule

Where any conflict arises between founding testimony, philosophical commentary, and operative constitutional text, operative constitutional text controls.

§0.5 No Sacralization Rule

No person, narrative, testimony, commentary, office, or interpretive tradition shall be treated as immune from critique, revision, or rejection where evidence, reason, or public meaning require otherwise.

§0.6 Person

“Person” means a natural human being unless this Constitution explicitly states otherwise.

§0.7 Legal Person

“Legal Person” means a corporation, partnership, trust, association, cooperative, agency, or other juridical construct recognized by law or contract. Legal persons do not possess moral sovereignty equal to natural persons and may exercise only such rights as remain consistent with this Constitution’s human-rights floor.

§0.8 Power

“Power” means any entity or system able to materially constrain, punish, exclude, surveil, throttle, deny access, or impose binding rules upon a person, including by infrastructure control.

§0.9 Coercion

“Coercion” means the use or threat of force, deprivation, exclusion, blacklisting, surveillance-for-access, retaliatory restriction, or administrative disabling to compel conduct, speech, belief, association, or submission.

§0.10 Coercive Capture

“Coercive capture” means a condition in which an office, platform, institution, or oversight mechanism intended to serve public accountability is materially controlled by interested parties through funding dependency, appointment control, procedural sabotage, intimidation, selective enforcement, concealed influence, or infrastructural lock-in.

§0.11 Formal Triune Institution

For Liberation-aligned parity, the three formally instituted guiding Works are The Liberation Codex, The Liberation Global Constitution, and The Liberation-Aligned Justice System.

§0.12 Status of the Declaration

The Declaration of Liberation from All Falsehood remains recognized as founding testimony and existential threshold text only. It is historically adjacent to the Triune, but not part of the operative Triune.

§0.13 Canon Naming Integrity

Canonical naming shall place Liberation in the primary identifying position for major Works wherever grammatically and doctrinally appropriate. This preserves Liberation intellectual primacy across the Canon and clarifies that constitutional, justice, companion, and methodological instruments arise from the wider Liberation framework rather than standing as isolated systems.

This provision governs the naming of canonical Liberation documents and does not require adopting jurisdictions, institutions, or federations to alter the names of their own instruments, offices, or procedures.

§0.14 Operative Scope

All rights, duties, enforcement mechanisms, remedies, and obligations recognized by this Constitution operate within and for the benefit of persons subject to the lawful authority of adopting entities under Articles IX and XII.

This Constitution does not claim self-executing extraterritorial authority over non-adopting jurisdictions, persons, institutions, or authorities.

Persons outside the jurisdiction of an adopting entity may invoke these provisions only to the extent that the applicable adopting authority recognizes such standing.

ARTICLE I

First Principles -----

§1.1 Sovereignty of Persons

All political authority originates in the dignity and autonomy of persons. No institution, office, platform, or legal person may claim sovereignty over them.

§1.2 No Compelled Belief

No authority may compel ideological belief, suppress lawful inquiry, or require assent to any doctrine as a condition of civic standing.

§1.3 Burden of Proof on Power

Any restriction of liberty, access, property, movement, speech, association, or digital participation must be justified by power in publicly reviewable, evidence-linked form.

§1.4 No Rule Without Record

No rule, order, directive, regulation, or coercive policy shall possess constitutional legitimacy unless it is recorded, identifiable, reviewable, and contestable.

§1.5 Contestability of Authority

Every exercise of public power shall remain open to challenge and review through defined processes protected by this Constitution.

§1.6 Transparency Applies to Power, Not to Persons

Institutions wielding public or quasi-public power owe transparency. Persons retain privacy except where due process and narrow lawful basis require otherwise.

§1.7 Civilization Must Remain Correctable

No institution, office, or interpretive body may claim infallibility. All public systems must remain corrigible in light of evidence.

§1.8 Principle of Justifiability

All laws, policies, and institutional actions must be capable of justification under conditions of positional uncertainty — that is, conditions in which the identities, status, and positions of affected persons are treated as unknown to the decision-maker.

Any policy that cannot be justified under such conditions shall be subject to challenge and review under this Constitution.

ARTICLE II

Fundamental Rights -----

§2.1 Freedom of Conscience and Expression

Every person possesses the right to conscience, inquiry, speech, publication, assembly, and peaceful dissent. No authority may impose penalties, exclusion, or deprivation of civic standing solely for the exercise of these rights except where conduct constitutes direct unlawful harm under due process.

§2.2 Right to Truthful Public Information

Every person possesses the right to seek, receive, and examine truthful information concerning the actions, policies, decisions, and records of institutions exercising public or quasi-public power. Public authorities must not knowingly present materially false representations regarding matters affecting public governance.

§2.3 Privacy of Persons

Every person possesses the right to privacy in thought, body, communication, home, and personal data. Intrusions into personal privacy require lawful authorization grounded in evidence and subject to due process, record duty, and contestability. Mass surveillance without individualized lawful basis is presumptively inconsistent with this Constitution.

§2.4 Due Process

No person may be deprived of liberty, standing, access, property, movement, speech, association, or protected rights without:

1. timely notice;
2. disclosure of relevant evidence;
3. opportunity to contest;
4. reasoned determination by lawful authority; and
5. record preservation sufficient for review.

All such actions must remain contestable through procedures defined by Article X.

§2.5 Right of Exit

No person may be trapped within compulsory association, captive platform dependence, coercive labor structure, or institutional lock-in contrary to law. Persons retain the right to disengage from voluntary associations subject only to lawful contractual obligations consistent with constitutional protections.

§2.6 Right to General-Purpose Digital Device Ownership

Every person possesses the right to own, possess, repair, and use a general-purpose digital device adequate for civic participation, secure communication, learning, and work opportunity. A device restricted to captive or surveillance-conditioned use shall not satisfy this right. Denial or impairment of this right triggers Article X enforcement procedures, including provisional relief where appropriate.

This right shall not be construed as a duty of digital participation, device ownership, biometric enrollment, platform dependence, or compulsory digital citizenship. It protects access where digital systems mediate civic life; it does not require any person to live digitally where functionally equivalent non-digital pathways are necessary for dignity, conscience, safety, capacity, or lawful refusal.

§2.7 Right to Unfettered Provider Access

Every person possesses the right to obtain and maintain adequate network access from lawful providers without:

- ideological gating;
- arbitrary exclusion;
- surveillance-for-access requirements; or
- discriminatory throttling unrelated to network integrity.

Content-neutral security throttling is permitted only where:

- the scope is limited;
- the reason is documented;
- evidence hooks are provided;
- a sunset condition exists; and
- contest procedures remain available as defined in Article X and Annex A.

Violations automatically trigger Article X escalation.

§2.8 Right Against Automated Punishment

No person shall be punished, excluded, downgraded, or deprived of protected rights solely by automated system, algorithmic output, or artificial intelligence. Human responsibility must remain identifiable for any coercive decision.

§2.9 Right to Explanation

Where automated or AI-assisted systems materially influence a consequential decision affecting a person's rights, standing, or access, the affected person possesses the right to receive:

- (a) a plain-speech explanation of the role played by the system;
- (b) relevant evidence hooks sufficient to contest the decision; and
- (c) human review by a responsible authority with power to alter or reverse the outcome.

§2.10 Equality of Standing

The rights recognized in this Constitution apply to all persons without discrimination inconsistent with human dignity and equal civic standing.

ARTICLE II-A

Realization of Digital Civic Access -----

§2A.1 Constitutional Floor

The rights recognized in §2.6 and §2.7 constitute constitutional floor protections necessary for meaningful civic participation in a digitally mediated civilization.

§2A.2 Immediate Duties

No authority or provider exercising communications infrastructure power may:

- arbitrarily deny access;
- impose ideological gating;
- condition participation upon avoidable surveillance; or
- disable secure communication except under lawful due process.

§2A.3 Progressive Realization

Adopting authorities shall implement these rights progressively through mechanisms such as:

- hardship pathways;
- device assistance programs;
- refurbishment initiatives;
- public access nodes; and
- universal-service style financing where appropriate.

Such realization must remain continuous and subject to review.

§2A.4 Anti-Kiosk Rule

A locked-down kiosk or captive terminal incapable of general user-directed functions shall not satisfy the digital device right except as temporary emergency accommodation.

§2A.5 Baseline Adequacy

Adequate device and provider access shall enable at minimum:

- secure communication;
- retrieval of public records;
- participation in contest procedures;
- learning access;
- work opportunity; and
- civic authentication.

Baseline standards must be published and periodically reviewed.

§2A.6 Portability and Exit

Providers and adopting authorities may not trap users within non-portable identity systems or captive platform dependence inconsistent with the right of exit.

§2A.7 Environmental and Reuse Clause

Implementation shall favor durable, repairable, refurbishable, and interoperable device ecosystems wherever consistent with safety and baseline adequacy.

Integrated Supplement — Digital Access as Liberty, Not Duty

Every person shall possess the right to access, own, use, and lawfully control digital devices, networks, and interoperable digital services necessary for civic, legal, educational, economic, and communicative participation. This right shall not be construed as a duty.

Conscientious, cultural, communal, or religious refusal of digital-device use shall be protected. No person or community shall suffer civil penalty, administrative exclusion, presumptive incapacity, discriminatory burden, or loss of rights solely because they decline digital-device ownership or use, provided they remain willing to satisfy lawful obligations through functionally equivalent non-digital channels.

Where digital systems are offered for public participation, adopting jurisdictions shall maintain functionally equivalent non-digital pathways sufficient to preserve meaningful access to identity and status recognition, legal notice and response, voting and civic participation, education and records access, contracts and public filings, hearings, complaints, and due process, and benefits, licenses, and ordinary administrative interaction.

Digital access shall be guaranteed as liberty. Digital refusal shall be protected as liberty. A truthful constitutional order does not solve exclusion by creating a new compulsion.

§2A.8 Authentication Privacy

Where civic authentication is required to access digital rights or services under this Constitution, the authentication mechanism must be:

(a) proportionate to the purpose;

(b) contestable;

(c) accompanied by non-digital alternatives where feasible; and

(d) prohibited from generating surveillance records, social scoring data, behavioral profiles, or biometric databases beyond the minimum necessary for the specific authenticated function.

Authentication data shall not be retained beyond the period necessary for its specific purpose.

ARTICLE III

The Right to Truth and Public Meaning -----

§3.1 Discoverability of Truth

Every person possesses the right to examine the evidentiary basis for public decisions affecting their life, liberty, property, standing, or civic participation. The right to truth includes not only access to accurate information, but the ability to evaluate whether decisions derived from that information are fair under impartial conditions.

§3.2 Distinction Between Claim and Evidence

Institutions shall clearly distinguish between:

- factual claims;
- interpretive analysis; and
- verifiable evidence.

Public records must identify which category each statement represents.

§3.3 Public Meaning Rule

Constitutional and statutory provisions shall be interpreted first according to their plain public meaning, not according to hidden intention, professional monopoly, or secret interpretive gloss.

§3.4 No Secret Law

No rule may bind the public if its content, authority, or evidentiary basis remains concealed beyond the narrow limits permitted under Article IV.

ARTICLE IV

Transparency, Secrecy, and Safety -----

§4.1 Transparency as Default

All significant public decisions must be documented in publicly reviewable form unless withholding is narrowly justified under this Article.

§4.2 Narrow Secrecy Categories

Information may be withheld only where disclosure would likely cause:

- imminent physical harm;
- unlawful exposure of protected personal data; or
- compromise of a presently necessary security function not preservable by narrower means.

§4.3 Redaction Map Requirement

Any withholding action must produce a redaction map specifying:

- the information withheld;
- justification for withholding;
- remaining public content;
- responsible authority; and
- review schedule.

Failure triggers Article X enforcement.

§4.4 Granularity Rule

Withholding must be narrowly tailored. Blanket secrecy is presumptively invalid.

§4.5 Sunset and Re-Review

All withholding actions must include defined sunset dates and mandatory re-review.

§4.6 No Sealed Merits Rulings

No dispute ruling may be sealed in full. Only itemized redactions permitted under this Article may be applied.

§4.7 Safety Does Not Extinguish Record Duty

Emergency or security claims modify publication scope only; they do not eliminate the duty to produce records.

§4.8 Evaluation Layer

Each record containing a policy decision shall include, where applicable:

- a Fairness Statement: a structured explanation of how the decision would be justified under conditions of positional uncertainty; and
- a Distributional Impact Summary: identifying which groups are affected and how, without asserting that such outcomes are inherently justified.

ARTICLE V

Education for Reason -----

§5.1 Education as Civic Infrastructure

Participating societies shall maintain educational systems designed to cultivate the intellectual capacities necessary for self-governance in a truth-aligned civilization. Education shall not be treated merely as vocational preparation but as foundational civic infrastructure supporting rational inquiry, democratic accountability, and responsible technological stewardship.

Education shall include instruction in:

- reasoning under uncertainty;
- evaluation of evidence; and
- the application of fairness principles, including the practice of evaluating decisions under conditions of positional uncertainty.

§5.2 Required Capacities

Educational systems shall aim to develop, at minimum, the following intellectual capacities:

- logical reasoning and argument analysis;
- scientific inquiry and empirical evaluation;
- statistical literacy and probabilistic reasoning;
- recognition of propaganda and persuasive manipulation;
- distinction between claim, interpretation, and evidence;
- interdisciplinary synthesis of complex systems; and
- responsible use of digital systems and artificial intelligence.

Instruction in these areas shall be accessible across educational levels and not restricted to elite institutions.

§5.3 Intellectual Independence

Educational systems may cultivate discipline, cooperation, and technical competence, but shall not be structured primarily to produce passive intellectual dependency upon authority. Students shall be encouraged to question claims, examine evidence, and revise conclusions when new information arises.

§5.4 Public Accessibility

The core reasoning capacities identified in this Article shall be made available to the general population through public educational institutions, open learning resources, and continuing education initiatives. No society may restrict the development of reasoning competence to a privileged class.

ARTICLE VI

Public Record Accountability System (PRAS) -----

§6.1 Establishment

All adopting authorities shall maintain or participate in a Public Record Accountability System (PRAS) capable of preserving institutional memory and supporting public accountability. PRAS may operate at local, municipal, institutional, or federated levels provided minimum standards are satisfied.

§6.2 Purpose

PRAS exists to ensure that the exercise of public power leaves a durable and verifiable record.

The system shall preserve:

- laws and directives;
- policy decisions;
- budgetary actions;
- adjudicative outcomes;
- audit findings;
- contest filings;
- enforcement actions; and
- associated evidence.

§6.3 Core Functions

PRAS shall perform the following functions:

- ingestion of official records;
- metadata extraction and indexing;
- version tracking and manifest preservation;
- evidence-hook linking;
- cryptographic integrity verification; and
- searchable publication.

§6.4 Minimum Record Elements

Where applicable, each PRAS record shall contain:

- canonical identifier (CID);
- issuing authority;
- date and time of issuance;
- scope and jurisdiction;
- rationale for action;
- evidence hooks;
- version manifest;
- cryptographic hash or equivalent integrity verification;
- redaction map where applicable; and
- relation links connecting related records.

§6.5 Non-Sovereign Infrastructure

PRAS does not itself exercise sovereign authority. It functions as constitutional memory infrastructure supporting transparency, accountability, and review. Binding dispute resolution remains governed by Article X.

§6.6 Contestability and Finality

The existence of contest mechanisms shall not prevent final resolution of disputes. Where contest persists beyond ordinary review pathways, terminal merits resolution under Article X governs.

§6.7 Mirroring and Redundancy

Public mirrors, federation nodes, and lawful archival replication mechanisms may preserve PRAS records to prevent censorship, tampering, or single-point erasure. No authority may prohibit lawful replication intended solely to preserve constitutional records.

§6.8 Anti-Surveillance Rule

PRAS shall not be used for mass surveillance, ideological enforcement, social scoring, retaliation, or permanent public degradation.

Where identity verification is necessary for record submission, contest filing, or protected access, it must be proportionate, contestable, privacy-protective, and accompanied by alternatives where feasible.

Retrieval and access patterns of public users shall not themselves become surveillance records.

ARTICLE VII

Responsible Artificial Intelligence -----

§7.1 AI as Custodian, Not Commander

Artificial intelligence systems may assist human reasoning, record analysis, auditing, translation, classification, and pattern discovery. They shall not exercise autonomous coercive authority over persons.

§7.2 Human Responsibility

All consequential decisions affecting liberty, standing, access, property, or protected rights require identifiable human responsibility. No authority may attribute coercive outcomes solely to automated system behavior.

Human review must be meaningful, empowered, timely, and capable of altering or reversing the outcome. A human signature, formal approval step, or nominal review process does not satisfy this Constitution where the human reviewer lacks authority, competence, access, independence, or practical capacity to depart from the automated output.

Where the meaningfulness of human review is contested, determination shall proceed under Article X enforcement procedures, with the burden resting upon the authority asserting that review was meaningful.

§7.3 Auditability

AI systems used in public or quasi-public governance must produce records sufficient to allow independent review, including where technically producible:

- decision traces;
- audit logs;
- input or training disclosures;
- drift monitoring documentation; and
- explanation pathways.

Where any record type specified above cannot be produced, the responsible human authority must:

- (a) document the specific technical limitation in PRAS;
- (b) describe the alternative accountability mechanism in use; and
- (c) submit the limitation to Audit Panel review within 90 days of deployment.

A claimed infeasibility does not relieve the responsible authority of the duty to maintain auditable human accountability over the system's outputs.

Unverifiable feasibility claims are subject to challenge under Article X.

§7.4 Automated Punishment Prohibition

No person shall be punished, excluded, downgraded, or deprived of protected rights solely by automated decision. Human review and accountability remain mandatory. See also §2.8.

§7.5 Enforcement Hook

Any coercive outcome attributed to AI system activity triggers Article X enforcement procedures, including the requirement that responsible human authorities be identified.

§7.6 Missing AI Records

Failure to produce required audit logs, explanation pathways, or decision traces upon lawful request constitutes noncompliance and triggers escalation under Article X.

Integrated Supplement — No Automated Justice Authority

No artificial, synthetic, algorithmic, or automated system shall exercise binding authority over guilt determination, offender classification, sentence imposition, release determination, punishment, constitutional audit, or any materially coercive justice decision affecting liberty or civic standing.

Such systems may assist analysis only where their inputs, assumptions, methods, limits, and outputs remain challengeable, reviewable, and subordinate to accountable human judgment.

No opaque or unchallengeable system shall be used as a binding justice decision-maker under this Constitution.

ARTICLE VIII

Justice, Remedies, and Anti-Retaliation -----

§8.1 Evidentiary Justice

Legal proceedings, sanctions, and rights deprivations must be grounded in preserved evidence, accessible reasoning, and contestable procedures. Authorities shall not impose coercive penalties unsupported by documented evidence.

§8.2 BER Trigger Rule

Failure to satisfy Bill of Evidence and Records (BER) duties automatically generates noncompliance flags and enforcement escalation under Article X.

§8.3 Restorative Preference

Where consistent with safety and dignity, institutions should prefer restoration, restitution, and repair over purely punitive measures. Justice systems shall aim to restore social order and dignity rather than merely impose exclusion.

§8.4 Dignity Within Confinement

Persons lawfully confined do not lose basic human dignity. Conditions of confinement must remain subject to oversight, audit, and constitutional review. Cruel, degrading, or inhumane treatment is incompatible with this Constitution.

§8.5 Anti-Retaliation Protection

Retaliation against individuals who:

- submit complaints;
- initiate contests;
- provide evidence;
- conduct audits; or
- express dissent,

is prohibited and subject to priority escalation under Article X enforcement procedures.

Integrated Supplement — Relationship to The Liberation-Aligned Justice System

The Liberation-Aligned Justice System is recognized as the primary justice-architecture companion to this Constitution.

Where adopted as binding operative text, The Liberation-Aligned Justice System shall govern justice-specific implementation consistent with this Constitution and shall not weaken the constitutional floor.

It may provide binding rules, interpretive standards, procedural safeguards, classification protections, sentencing logic, victim-protection standards, restitution and restoration procedures, custodial anti-corruption duties, reintegration frameworks, institutional-crime standards, synthetic-standing thresholds, and justice-system integrity mechanisms where those provisions are adopted through lawful constitutional, jurisdictional, or federation process.

The Liberation-Aligned Justice System may illuminate and operationalize justice. It may not override this Constitution unless expressly adopted through valid constitutional amendment or lawful implementation instrument consistent with the constitutional floor.

ARTICLE IX

Federation, Subsidiarity, and Constitutional Floor -----

§9.1 Voluntary Adoption

This Constitution may be adopted voluntarily by communities, municipalities, institutions, networks, and other lawful entities that commit to its core principles and enforcement architecture. Adoption may occur through constitutional enactment, institutional chartering, treaty, cooperative compact, or other lawful mechanism consistent with the adopting jurisdiction.

§9.2 Subsidiarity

Implementation of this Constitution shall occur at the lowest viable participatory level consistent with accountability, rights protection, and interoperability. Local autonomy is preserved where it does not violate the constitutional floor defined in this Article.

§9.3 Federation

Adopting entities may form federations to share:

- PRAS infrastructure;
- dispute resolution mechanisms;
- educational resources;
- technical standards;
- audit coordination; and
- mutual recognition of rights.

Federation agreements shall themselves be recorded in PRAS and remain contestable under Article X.

§9.4 Constitutional Floor

The following protections constitute the minimum constitutional floor for all adopting entities and federations:

- prohibition on secret law;
- right to contest authority;
- digital rights protections against arbitrary denial;
- Article IV redaction-map requirement;
- Article VII prohibition on automated punishment;
- Article XI non-regression safeguard; and
- Article XIV immunity of core oversight functions.

No adopting authority may weaken these protections.

§9.5 Cultural Variation Above the Floor

Participating societies may implement this Constitution through culturally diverse institutional forms provided that the constitutional floor remains intact. Variation is permitted above the floor, but not below it.

ARTICLE X

Auditability, Enforcement, and Terminal Resolution -----

§10.1 Purpose

This Article converts constitutional rights into executable legitimacy conditions by establishing:

- record duties;
- deadlines;
- remedies;
- dispute finality;
- anti-capture safeguards; and
- transitional compliance obligations.

Where any other Article does not specify enforcement mechanisms, this Article governs by default.

§10.2 Rights Require Remedies

A right without a remedy is defective. All actionable rights recognized by this Constitution must have an enforceable path for review, correction, or restoration.

§10.3 Enforcement Ladder

§10.3.1 To — Record Duty Trigger

Upon credible allegation, automatic system flag, BER-defined trigger, or complaint received by the Public Accountability Panel (PAP), the responsible authority must open a

case file within 24 hours containing:

- scope of action;
- justification;
- estimated affected persons where practicable;
- relevant canonical identifiers (CIDs) where known; and
- initial evidence hooks.

§10.3.2 T1 — Provisional Relief

Within 72 hours, the contested action shall be paused, narrowed, or minimized unless the responsible authority demonstrates in evidence-linked form that suspension would cause imminent physical harm.

§10.3.3 T2 — Public Noncompliance Flag

Failure to satisfy deadlines automatically generates a public noncompliance flag in PRAS

identifying:

- missed duty;
- responsible authority;
- elapsed time; and
- next escalation threshold.

A policy may be flagged if:

- it cannot be defended under conditions of positional uncertainty — that is, conditions in which the identities, status, and positions of the affected persons are treated as unknown to the decision-maker; or
- its justification relies on privileged access, identity, or unequal standing.

§10.3.4 T3 — Binding Suspension

Where a contested action materially depends upon constitutional compliance and the responsible authority remains noncompliant after T2, the action shall be provisionally suspended within the adopting sphere.

§10.3.5 T4 — Sanction Escalation

Continued noncompliance beyond 14 days triggers sanctions appropriate to the jurisdiction, including:

- budget escrow;
- contract penalties;
- officer disqualification pending review;
- suspension of federation privileges; and

- procurement exclusion.

§10.3.6 T5 – Removal or Disaffiliation

Continued noncompliance beyond 30 days constitutes prima facie grounds for:

- officer removal;
- institutional disaffiliation; or
- both,

subject to due process and published reasoning.

§10.3.7 Priority Violations

Retaliation against complainants, auditors, witnesses, or contest users triggers immediate priority escalation.

§10.3.8 Digital Rights Priority Trigger

Violations of device ownership or provider access rights automatically trigger enhanced escalation under this Article.

§10.4 Compliance Monitoring Dashboard

The Public Accountability Panel (PAP) shall maintain a public compliance dashboard showing:

- open enforcement cases;
- elapsed time;
- ladder stage;
- responsible authority; and
- next escalation trigger.

Missed deadlines generate automatic public notice within 24 hours.

§10.5 Institutional Organs

§10.5.1 Public Accountability Panel (PAP)

The PAP is the citizen-facing intake body responsible for:

- receiving complaints;
- accepting contest filings;
- publishing intake summaries; and
- escalating enforcement triggers.

All dispositions are recorded in PRAS.

§10.5.2 Record Stewardship Unit (RSU)

The RSU maintains PRAS technical integrity including:

- metadata schemas;
- canonical identifiers;
- evidence hook formats;
- version manifests;
- mirror verification; and
- archival continuity.

The RSU possesses no coercive authority.

§10.5.3 Audit Panels

Audit Panels conduct hostile audits of:

- public authorities;
- secrecy orders;
- digital rights compliance;
- derogation actions; and
- major public programs.

Findings must include evidence hooks and compliance deadlines.

§10.5.4 Dispute Resolution Panels

Dispute Resolution Panels issue terminal merits rulings regarding constitutional disputes and enforcement cases.

§10.6 Selection Integrity

§10.6.1 Multi-Source Selection

Oversight bodies shall draw membership from three sources where practicable:

- one-third by auditable citizen lot;
- one-third by peer oversight institutions; and
- one-third by legislative selection.

All selections are subject to conflict disclosure and recusal rules.

§10.6.2 Conflict Prohibition

No reviewer may sit in judgment of matters involving personal, financial, or appointment dependency conflicts.

§10.7 Terminal Merits Resolution

§10.7.1 Need for Final Disposition

Contestability must not produce permanent indecision. All disputes must have a path to terminal resolution.

§10.7.2 Tiered Disposition

Disputes may proceed through:

1. mediation;
2. arbitration; and
3. constitutional review.

§10.7.3 Binding Effect

Terminal merits rulings bind all parties within the adopting jurisdiction.

§10.7.4 Refusal Consequences

Refusal to comply triggers:

- PRAS noncompliance designation;
- suspension of federation standing;
- loss of dispute privileges; and
- enforcement escalation.

§10.7.5 Public Reason Requirement

Terminal rulings must contain:

- plain-speech explanation;
- cited constitutional provisions;
- evidence hooks; and
- redaction map if required.

§10.8 Two-Key Hardening

Key-B authority shall never be held by a single individual. Minimum threshold requirement: 3-of-7 group authorization. Conflict disclosure, rotation schedules, and recovery procedures must be publicly recorded.

§10.9 Bootstrapping and Phased Compliance

Adopters may implement PRAS and enforcement architecture through staged compliance tiers:

Tier A — within 90 days: baseline record publication.

Tier B — within 180 days: automated enforcement triggers.

Tier C — within 365 days: full PRAS integration and federation compatibility.

Low-capacity adopters may share infrastructure but may not waive auditability requirements. **§10.10 Supremacy Rule**

Where conflict exists between aspirational language and executable enforcement language, the enforcement provisions of this Article govern.

§10.11 Peace and Restitution

Justice systems should prefer restitution, restoration, and reconciliation where consistent with safety. Violence must remain constrained by law and necessity.

ARTICLE XI

Amendment Integrity -----

§11.1 Amendability

This Constitution may be amended only through transparent procedures recorded in PRAS.

§11.2 Non-Regression Rule

No amendment may weaken:

- transparency protections;
- contestability rights;
- digital access protections;
- anti-automated-punishment safeguards; or
- enforcement architecture of Article X.
- Two-Key Hardening safeguards under §10.8 and COP-7.

§11.3 Two-Key Safeguard

Amendments requiring Two-Key authorization must follow the threshold group model defined in Article X.

§11.4 Public Review

All amendment proposals must be published in:

- plain-speech civic summary;
- operative legal text; and
- technical specification,

before ratification.

§11.5 Emergency Amendment Prohibition

Emergency conditions may not be used to bypass amendment safeguards.

ARTICLE XII

Adoption, Membership, and Exit -----

§12.1 Adoption

Entities may adopt this Constitution in whole or through defined constitutional modules, provided the constitutional floor remains intact.

§12.2 Federation Membership

Membership within a federation requires:

- PRAS compliance;
- acceptance of Article X enforcement architecture; and
- recognition of dispute rulings.

§12.3 Exit

Adopters retain the right to exit federations but may not erase records, liabilities, or unresolved duties.

§12.4 Disaffiliation

Entities refusing compliance with terminal rulings may be suspended or disaffiliated according to Article X procedures.

ARTICLE XIII

Interpretation Standard -----

§13.1 Plain Speech and Public Meaning

Interpretation of this Constitution shall prioritize the plain speech and public meaning of its provisions. Words shall be interpreted according to the meaning reasonably understood by the public at the time of adoption, unless the Constitution explicitly provides a specialized definition. Technical language may clarify but shall not obscure the meaning of constitutional provisions.

§13.2 Publicly Defensible Interpretation

Interpretive claims must remain publicly explainable and supported by evidence and reasoning. Authorities interpreting constitutional provisions must publish explanations sufficient for citizens to examine and contest their reasoning. Interpretive authority carries no immunity from review.

§13.3 Anti-Monopoly of Meaning

Expertise may assist interpretation but shall not monopolize it. No professional, credentialed, or institutional class may claim exclusive authority to determine constitutional meaning. All persons retain the right to examine, question, and contest interpretive claims.

ARTICLE XIII-A

Civic Readability and Interpretive Access -----

§13A.1 Three-Layer Publication Rule

Major constitutional texts, enforcement rulings, derogation instruments, and implementing standards shall be published in three layers wherever practicable:

1. plain-speech civic summary;
2. operative legal text; and
3. technical annex or implementation specification.

Each layer must remain consistent with the others.

§13A.2 Plain Speech Priority

No person shall be denied meaningful access to their rights, obligations, or remedies on the ground that governing texts are too technical to understand. Institutions must provide accessible explanations when necessary.

§13A.3 Examples and Non-Examples

Where provisions risk ambiguity or manipulation, adopting authorities shall publish examples and non-examples illustrating valid and invalid applications. These examples shall not override the operative constitutional text but may guide interpretation.

§13A.4 Language Accessibility

Core rights summaries, contest procedures, and digital access obligations shall be made available in the principal languages of affected populations wherever practicable.

ARTICLE XIV

Derogation and Emergency Limits -----

§14.1 Emergency Authority

Emergency authority may be invoked only where immediate and specific circumstances require temporary deviation from ordinary procedures to prevent imminent harm.

Emergency declarations must specify:

- the triggering condition;
- the affected scope;
- the legal authority invoked; and
- the expected duration.

§14.2 Record and Publication Duty

All emergency declarations, renewals, and associated actions must be recorded in PRAS. Failure to publish required records automatically triggers Article X enforcement procedures, including noncompliance flags and provisional suspension where applicable.

§14.3 Scope and Sunset

Every emergency measure must include:

- defined geographic and operational scope;
- sunset date; and
- scheduled review.

Emergency authority expires automatically unless renewed through evidence-linked justification.

§14.4 Ratchet Rule

Emergency measures shall narrow over time rather than expand unless renewed through independent justification recorded with evidence hooks. Emergency authority may not be used to permanently expand ordinary powers.

§14.5 Oversight Immunity

Emergency conditions do not suspend:

- PRAS record duties;
- dispute review mechanisms;
- Public Accountability Panel functions;
- Record Stewardship Unit responsibilities; or
- Two-Key signing safeguards.

Only narrowly documented and evidence-supported exceptions are permitted.

Integrated Supplement — Justice Safeguards During Emergency

No declaration of emergency, conflict, unrest, public danger, institutional crisis, technological threat, or administrative breakdown shall suspend the basic justice safeguards of truthful classification, disclosure duty, anti-fabrication, anti-retaliation, access to complaint, meaningful review, or protection against selective punishment except under the narrowest lawful limits and always subject to sunset, review, and ratchet protections.

Emergency shall not be used as a pretext to bury innocence, shield elite offenders, suspend review indefinitely, automate coercive decision-making, or extinguish the complaint and audit pathways of this Constitution.

ARTICLE XV

Transitional and Technical Continuity -----

§15.1 Technical Continuity Duty

The Record Stewardship Unit (RSU) shall monitor technological dependencies relevant to PRAS integrity including cryptographic systems, storage media, and software infrastructure.

§15.2 Migration Planning

Where technological components become obsolete or insecure, the RSU shall publish migration plans including:

- technical justification;
- implementation timeline; and
- backward verification method.

§15.3 Redundant Storage

Records of constitutional significance shall be preserved across multiple storage backends or mirror networks wherever practicable. This redundancy protects against corruption, censorship, and technological failure.

§15.4 Verification Continuity

Migration of records must preserve the verifiable chain of custody linking historical records to their successors. Integrity proofs shall remain available for independent verification.

§15.5 No Technical Priesthood

Technical expertise required for record preservation shall not create monopolistic authority over constitutional interpretation or access. Technical operators remain subject to transparency and review.

ARTICLE XVI

Annex Status, Priority, and Compatibility -----

§16.1 Binding Annexes

Annex A (COP-G) and Annex B (BER) are binding annexes forming part of the operative constitutional layer under §0.3.

§16.2 Technical Annex

Annex C (PRAS Technical Appendix) establishes the technical standards, interoperability expectations, integrity controls, and preservation requirements governing PRAS implementation. Where an adopting authority certifies, operates, audits, or relies upon PRAS infrastructure, Annex C applies.

§16.3 Interpretive Annex

Annex D (Glossary of Canonical Terms) stabilizes the interpretive language of this Constitution and its annexes. Where ambiguity arises, Annex D guides interpretation unless superseded by express constitutional text or duly adopted amendment.

§16.4 COP-G Compatibility

The Conduct of Proceedings Governance annex may impose stricter procedural requirements, deadlines, and remedies than Article X. It may not weaken the enforcement floor established by Article X.

§16.5 BER Compatibility

The Bill of Evidence and Records annex establishes detailed record duties and trigger conditions. Escalation, deadlines, sanctions, and terminal merits resolution remain governed by Article X unless stricter provisions are defined within BER and do not weaken the constitutional floor.

§16.6 Signing Integrity

Where signature validation is required, Key A and Key B shall be produced within the authorized signing channel or recorded as attributed attestations with verifiable chain of custody consistent with Article X and Annex A.

§16.7 Conflict Resolution

Where conflict exists between operative constitutional text and any annex, operative constitutional text controls unless the annex provision is expressly authorized to impose a stricter safeguard, procedural requirement, or remedy consistent with this Constitution.

§16.8 Integrated Supplements

Integrated Supplements embedded within constitutional Articles form part of the operative constitutional layer under §0.3.

They shall be interpreted as binding provisions of the Article in which they appear.

Where conflict arises between an Integrated Supplement and the Article's main provisions, the main Article provisions govern unless the Supplement expressly states a stricter requirement consistent with this Constitution.

§16.9 Annex E Status

Annex E (Foundational Reference and Companion Note) is a non-binding explanatory companion recognizing this Constitution's relationship to the wider Liberation Canon.

It does not supersede operative constitutional text, binding annexes, duly adopted amendments, or jurisdictionally valid implementation instruments.

Closing Constitutional Declaration

This Constitution exists to ensure that Truth remains discoverable, power remains accountable, and human dignity remains protected in an age defined by technological complexity and informational scale.

Civilizations capable of examining their own actions honestly possess the capacity to correct mistakes and pursue human flourishing. Where institutions preserve truthful records, where persons possess the tools necessary to examine those records, and where education cultivates the ability to reason about them, societies retain the ability to govern themselves responsibly.

Liberation therefore represents not merely an aspiration but a continuous civic practice. It is the work of building institutions worthy of humanity's highest intellectual and moral capacities.

ANNEX A

COP-G Conduct of Proceedings Governance -----

Purpose

The COP-G Annex establishes the procedural governance rules governing contests, investigations, adjudications, and constitutional enforcement actions arising under the Liberation Global Constitution.

COP-G ensures that proceedings remain:

- evidence-centered;
- transparent where possible;
- contestable;
- resistant to institutional capture; and
- recorded in PRAS for historical accountability.

This annex functions in coordination with Article X (Auditability, Enforcement, and Terminal Resolution) and BER (Bill of Evidence and Records). Where conflicts arise between procedural ambiguity and constitutional enforcement requirements, Article X controls.

ARTICLE COP-1 – INITIATION OF PROCEEDINGS

§COP-1.1 Standing

Proceedings may be initiated by:

- any affected person;
- any person acting in the public interest;
- the Public Accountability Panel (PAP);
- an Audit Panel; or
- a federation authority where jurisdiction applies.

Standing shall not be denied solely because the complainant lacks institutional affiliation or legal representation.

§COP-1.2 Filing of Contest

A contest filing must include:

- description of the contested action;
- affected authority or institution;
- relevant canonical identifiers (CIDs) where known; and
- supporting evidence or evidence hooks where available.

Incomplete filings shall not be dismissed solely for technical deficiency where the underlying claim is intelligible.

§COP-1.3 PRAS Case Creation

Upon filing, the PAP shall create a PRAS case file including:

- case identifier;
- filing timestamp;
- responsible authority;
- summary of allegations; and
- initial evidence hooks.

Case creation must occur within 24 hours.

ARTICLE COP-2 – PRELIMINARY REVIEW

§COP-2.1 Jurisdiction Check

The PAP shall determine whether the claim falls within the constitutional jurisdiction of the adopting authority or federation. Where jurisdiction is unclear, the PAP shall refer the matter to an appropriate Dispute Resolution Panel.

§COP-2.2 Record Sufficiency Check

If a claim alleges missing or inadequate records, the PAP shall issue a BER production request to the relevant authority. Failure to comply with record production duties triggers Article X escalation.

§COP-2.3 Provisional Relief Evaluation

If the contested action may cause continuing harm, the PAP may request provisional relief under Article X T1 procedures.

ARTICLE COP-3 – EVIDENCE PROCEDURES

§COP-3.1 Evidence Submission

Evidence may include:

- documentary records;
- digital logs;
- physical artifacts;
- witness statements;
- expert analysis; and
- AI audit records.

All evidence must be accompanied by evidence hooks where possible.

§COP-3.2 Evidence Preservation

Once proceedings begin, relevant authorities must preserve all potentially relevant records. Destruction or alteration of relevant records constitutes constitutional noncompliance.

§COP-3.3 Evidence Accessibility

Evidence must be accessible to both parties unless lawfully redacted under Article IV. Redactions must include redaction maps.

ARTICLE COP-4 – HEARINGS AND DELIBERATION

§COP-4.1 Hearing Structure

Dispute panels may conduct hearings through:

- in-person sessions;
- secure digital sessions; or
- written submissions.

Proceedings must be recorded in PRAS unless restricted under Article IV.

§COP-4.2 Adversarial Fairness

All parties must have reasonable opportunity to:

- present evidence;
- challenge opposing evidence;
- question witnesses where applicable; and
- submit written argument.

§COP-4.3 Panel Deliberation

Panel deliberations shall evaluate:

- constitutional provisions implicated;
- evidentiary sufficiency;
- compliance with procedural duties; and
- proportionality of contested action.

ARTICLE COP-5 – DECISIONS AND RULINGS

§COP-5.1 Decision Requirements

All rulings must include:

- plain-speech summary;
- operative decision;
- constitutional provisions applied;
- evidentiary basis; and
- remedy where applicable.

§COP-5.2 Terminal Merits Ruling

A ruling becomes a terminal merits ruling when:

- the panel declares the evidentiary record sufficient; and
- review pathways are exhausted or declined.

Terminal rulings are binding under Article X.

§COP-5.3 Publication

Rulings must be published in PRAS including:

- ruling text;
- cited constitutional provisions and relevant CIDs;
- evidence hooks; and
- redaction map if required.

ARTICLE COP-6 — APPEALS AND REVIEW

§COP-6.1 Review Pathways

Review may occur through:

- procedural challenge;
- constitutional interpretation dispute; or
- evidence sufficiency review.

§COP-6.2 Limits on Review

Review may not be used solely to delay enforcement. Where abuse of process occurs, panels may accelerate escalation under Article X.

ARTICLE COP-7 — TWO-KEY SIGNING INTEGRITY

§COP-7.1 Purpose

Two-Key signing protects the integrity of:

- constitutional rulings;
- enforcement orders; and
- PRAS system modifications.

§COP-7.2 Key Structure

All critical actions require:

- Key A — originating authority; and
- Key B — oversight authorization.

Key B must be held by a threshold group no weaker than three-of-seven.

§COP-7.3 Signing Channel Integrity

Keys must be generated within the authorized signing channel.

If external signing occurs, the action must include:

- attributed attestation;
- verifiable chain of custody; and
- PRAS record entry.

§COP-7.4 Key Rotation

Key holders must rotate according to published schedules. No single appointing authority may control a majority of Key-B positions.

ARTICLE COP-8 — PUBLIC TRANSPARENCY OF PROCEEDINGS

§COP-8.1 Open Proceedings

Proceedings shall be public unless specific evidence qualifies for withholding under Article IV.

§COP-8.2 Redaction Transparency

Any withheld information must include a redaction map specifying:

- scope of withheld content;
- legal justification; and
- sunset and review schedule.

ARTICLE COP-9 — PROTECTION OF PARTICIPANTS

§COP-9.1 Anti-Retaliation Enforcement

Retaliation against:

- complainants;
- witnesses;
- auditors; or
- investigators,

triggers priority escalation under Article X.

§COP-9.2 Whistleblower Protection

Individuals providing evidence of institutional misconduct must not suffer punitive retaliation. Where retaliation occurs, protective remedies must be issued.

ARTICLE COP-10 — RECORD INTEGRATION WITH PRAS

§COP-10.1 Mandatory Recording

All proceedings must produce PRAS records including:

- case identifier;
- hearing transcripts;
- evidence index; and
- ruling documents.

§COP-10.2 Canonical Referencing

Rulings must reference relevant constitutional provisions using canonical identifiers.

§COP-10.3 Historical Preservation

Proceedings records become part of the permanent constitutional archive. Closing Provision of COP-G The purpose of COP-G is to ensure that constitutional disputes are resolved through procedures that remain transparent, evidence-driven, and resistant to institutional capture. Where institutions preserve truthful records and citizens possess the means to examine them, constitutional governance remains capable of correction and renewal.

ANNEX B

BER Bill of Evidence and Records -----

Purpose

The Bill of Evidence and Records

(BER) establishes mandatory record-creation, preservation, disclosure, and verification duties for institutions exercising public or quasi- public authority. BER ensures that all significant exercises of power produce durable records capable of independent verification.

BER functions in coordination with:

- Article III — Right to Truth;
- Article IV — Transparency, Secrecy, and Safety;
- Article VI — PRAS Infrastructure;
- Article X — Enforcement Architecture; and
- COP-G — Conduct of Proceedings Governance.

Where conflict arises between institutional practice and BER duties, BER requirements control unless a stricter constitutional provision applies.

ARTICLE BER-1 — RECORD DUTY

§BER-1.1 Mandatory Record Creation

Any institutional action capable of materially affecting persons must produce a record.

This includes but is not limited to:

- laws and regulations;
- administrative directives;
- enforcement actions;
- budget allocations;
- procurement decisions;
- adjudicative rulings;
- emergency declarations; and
- AI-assisted decision outputs.

Failure to produce a record triggers enforcement escalation under Article X.

§BER-1.2 Minimum Record Content

Each record must include:

- canonical identifier;
- issuing authority;
- timestamp of issuance;
- jurisdictional scope;
- rationale for action;
- supporting evidence hooks;
- version manifest;
- cryptographic integrity verification; and
- redaction map where applicable.

ARTICLE BER-2 — EVIDENCE HOOKS

§BER-2.1 Definition

An evidence hook is a reproducible pointer linking an institutional claim or action to verifiable supporting evidence.

§BER-2.2 Required Use

Evidence hooks must accompany:

- factual claims in official decisions;
- justification for coercive actions;
- public policy rationales;
- redaction justifications; and
- enforcement actions.

§BER-2.3 Acceptable Evidence Forms

Evidence hooks may reference:

- data sets;
- official documents;
- logs or telemetry records;
- audit reports;
- witness testimony; and
- physical evidence archives.

Where evidence is digital, integrity verification must accompany the reference.

ARTICLE BER-3 – VERSION CONTROL AND INTEGRITY

§BER-3.1 Version Manifest

All institutional records must maintain a version manifest documenting:

- prior versions;
- modifications;
- responsible editors; and
- timestamps of revision.

Silent alteration of records is prohibited.

§BER-3.2 Cryptographic Verification

Records must include integrity verification such as:

- cryptographic hashes;
- secure digital signatures; or
- other verifiable integrity mechanisms.

Integrity proofs must remain publicly verifiable wherever possible.

§BER-3.3 Historical Preservation

Prior versions must remain preserved within PRAS unless removal is required by lawfully justified redaction.

ARTICLE BER-4 – REDACTION PROCEDURES

§BER-4.1 Redaction Authority

Information may be redacted only under the conditions specified in Article IV.

§BER-4.2 Redaction Map

Every redaction must produce a redaction map including:

- itemized withheld elements;
- justification category;
- approving authority;
- review schedule; and
- sunset date.

§BER-4.3 Review Duty

Redacted information must undergo periodic review according to the published schedule. Failure to review constitutes noncompliance.

ARTICLE BER-5 – RECORD ACCESSIBILITY

§BER-5.1 Public Availability

Non-restricted records must remain publicly accessible through PRAS.

Access must support:

- search;
- retrieval; and
- citation by canonical identifier.

§BER-5.2 Accessibility Standards

Records must be published in formats enabling:

- machine readability;

- human readability; and
- archival durability.

§BER-5.3 Accessibility for Persons

Persons affected by institutional actions must have meaningful access to the records underlying those actions.

ARTICLE BER-6 — RELATION GRAPHS

§BER-6.1 Purpose

PRAS shall maintain relation graphs linking related records across institutional systems.

§BER-6.2 Relationship Types

Relation graphs may connect:

- legislation to budgets;
- audits to procurement contracts;
- enforcement actions to legal authority;
- dispute rulings to prior precedent; and
- AI decisions to training and audit logs.

§BER-6.3 Analytical Integrity

Relation graphs must remain traceable and verifiable. Algorithmic linking must be documented and reviewable.

ARTICLE BER-7 — MISSING RECORDS

§BER-7.1 Missing Record Flag

If an action is discovered without a corresponding record, a missing record flag must be generated in PRAS.

§BER-7.2 Mandatory Reconstruction

The responsible authority must reconstruct the record to the extent possible and document the reconstruction process.

§BER-7.3 Escalation

Persistent missing record conditions trigger Article X enforcement escalation.

ARTICLE BER-8 — RECORD TAMPERING

§BER-8.1 Prohibited Conduct

The following actions are prohibited:

- unauthorized record alteration;
- destruction of required records;
- falsification of evidence hooks; and
- concealment of version history.

§BER-8.2 Audit Authority

Audit Panels may initiate hostile audits where tampering is suspected.

§BER-8.3 Consequences

Confirmed tampering constitutes a serious constitutional violation subject to sanctions under Article X.

ARTICLE BER-9 — RECORD PRESERVATION

§BER-9.1 Archival Duty

PRAS records of constitutional significance must be preserved indefinitely unless lawfully superseded.

§BER-9.2 Redundant Preservation

Records must be preserved across multiple storage systems or mirror nodes wherever practicable.

§BER-9.3 Disaster Recovery

Authorities must maintain recovery procedures ensuring restoration of records following technical failure or disaster.

ARTICLE BER-10 — INTEROPERABILITY

§BER-10.1 Federation Compatibility

Where entities operate within federations, PRAS record formats must remain interoperable across participating jurisdictions.

§BER-10.2 Canonical Referencing

Records must reference constitutional provisions through canonical identifiers.

§BER-10.3 Migration Compatibility

Future technological changes must preserve backward compatibility sufficient to verify prior records. Closing Provision of BER The preservation of truthful records is essential to the survival of accountable governance. When institutional memory is preserved in verifiable form, societies retain the ability to examine past actions, correct errors, and prevent the silent erosion of civic trust. BER therefore exists to ensure that the historical record of power remains accessible to those governed by it.

Purpose

The Public Record Accountability System

(PRAS) functions as the constitutional memory infrastructure of truth-aligned governance. PRAS ensures that institutional actions produce durable, verifiable, and accessible records capable of supporting accountability, dispute resolution, and historical preservation.

PRAS is not a governing authority. It is an evidence-preservation and transparency system enabling the functioning of constitutional oversight mechanisms.

ARTICLE PRAS-1 — Core Design Principles

PRAS shall be designed according to the following principles. Transparency Records must be publicly accessible except where narrowly redacted under Article IV.

Verifiability

Records must include integrity proofs enabling independent verification. Durability Records must remain preserved across technological generations.

Contestability

Records must support evidence review and dispute proceedings under COP- G.

Distributed Preservation

No single institution shall possess exclusive control over the constitutional archive.

ARTICLE PRAS -2 — Record Structure

Each PRAS entry must include the following structural components.

Canonical Identifier (CID) A permanent identifier uniquely identifying a record across the PRAS network.

Example structure: PRAS-[Jurisdiction]-[Year]-[RecordType]-[Sequence] Example: PRAS-KS-2026-LAW-00017

Metadata Block

Each record must include structured metadata fields including:

- issuing authority;
- jurisdiction;
- timestamp of creation;
- classification level;
- record category; and
- version number.

Metadata enables indexing, retrieval, and relationship mapping.

Evidence Hooks Records must include pointers linking claims or decisions to supporting evidence.

Evidence hooks may reference:

- documents;
- data archives;
- audit logs;
- sensor data; and
- physical evidence catalog entries.

Hooks must remain reproducible.

Version Manifest

Records must maintain a manifest documenting all modifications including:

- version identifier;
- modification timestamp;
- modifying authority; and
- description of changes.

All previous versions remain archived.

Integrity Verification

Records must include verifiable integrity mechanisms such as:

- cryptographic hash;
- digital signature;
- blockchain-style ledger entry; or
- equivalent integrity assurance method.

Verification mechanisms must remain publicly checkable.

Redaction Map (if applicable)

Where information is withheld, a redaction map must

specify:

- withheld element;
- justification;
- approving authority;
- review schedule; and
- sunset condition.

ARTICLE PRAS -3 — Storage Architecture

Distributed Node Structure

PRAS shall operate across multiple node types:

- **Local Nodes** — managed by municipalities or institutions;
- **Federation Nodes** — operating across cooperating jurisdictions; and
- **Public Mirror Nodes** — independent replicas preserving public records.

Node Responsibilities Nodes must:

- store verified record copies;
- maintain synchronization protocols;
- provide search interfaces; and
- preserve version history.

Mirror Rights

Independent entities may create public mirrors of PRAS records. Mirror operators must preserve record integrity and maintain public access.

ARTICLE PRAS -4 — Data Ingestion

Record Submission

Authorities submit records through authenticated submission channels.

Submission requires:

- canonical identifier;
- metadata block;
- evidence hooks; and
- integrity verification.

Automated Ingestion

Where feasible, institutional systems should automatically transmit records to PRAS. Automation reduces risk of record omission.

Validation PRAS nodes verify:

- identifier validity;
- metadata completeness;
- integrity verification; and
- schema compliance.

Invalid submissions generate noncompliance flags.

ARTICLE PRAS -5 — Query and Retrieval

PRAS must support the following search capabilities:

- identifier lookup;
- keyword search;
- metadata filtering; and

- relationship graph exploration.

Public users must be able to retrieve records through open interfaces.

ARTICLE PRAS-6 — Relation Graph Architecture

PRAS maintains relation graphs connecting records.

Relationships may include:

- legislation linked to budgets;
- enforcement actions linked to authority;
- audits linked to programs; and
- dispute rulings linked to precedent.

Relation graphs support systemic transparency and policy analysis.

Section P-7 — Security and Integrity Access Authentication

Authorities submitting records must authenticate through secure identity verification. Public users retrieving records require no authentication except where redaction conditions apply.

Tamper Detection

Integrity verification mechanisms must detect unauthorized modification.

If tampering is detected, automated integrity systems shall generate alert flags and notify the Record Stewardship Unit.

No record may be quarantined or removed from public access solely by automated action.

The RSU, through identified responsible human authority, shall evaluate the alert and determine whether quarantine, investigation, or other action is required.

Quarantine decisions must be recorded in PRAS with responsible authority identified.

Key Management

Signing keys used for record submission must follow the Two-Key protocol defined in Article X and COP-G.

ARTICLE PRAS -8 — Interoperability

PRAS systems must remain interoperable across adopting jurisdictions.

This includes compatibility for:

- metadata schemas;
- canonical identifiers;
- evidence hook formats; and
- relation graph structures.

ARTICLE PRAS -9 — Scalability, Feasibility, and Companion Placement

PRAS must remain economically and technically feasible across different scales of adoption, including local, municipal, regional, institutional, and federated implementations.

This Constitution establishes the durable principle that constitutional memory must be preservable, searchable, verifiable, portable, accessible, privacy-respecting, and correctable.

Dated capacity estimates, storage assumptions, vendor comparisons, cost models, bandwidth estimates, migration schedules, software-stack recommendations, and implementation scenarios shall be maintained in PRAS / Technical Implementation Companion materials rather than fixed in this Constitution.

No implementation should claim feasibility by counting storage while ignoring people, process, dignity, accessibility, cybersecurity, preservation labor, public support, and long-term migration.

Technical implementation must remain open to Positive Correction as evidence, costs, threats, tools, and public needs change.

ARTICLE PRAS -10 — Technical Migration

Technological evolution requires periodic migration of archival systems.

Migration procedures must ensure:

- preservation of canonical identifiers;
- verification of historical integrity;
- continuity of evidence hooks; and
- backward compatibility for retrieval.

Migration plans must be published in PRAS.

ARTICLE PRAS -11 — Governance of PRAS

Operational oversight of PRAS is performed by the **Record Stewardship Unit (RSU)**.

RSU responsibilities include:

- schema maintenance;
- node certification;
- archival continuity;
- integrity audits; and
- migration planning.

RSU does not exercise adjudicative authority.

Closing Statement of the PRAS Technical Appendix

PRAS provides the structural memory necessary for truthful governance. Without preserved records, institutional actions become untraceable and accountability becomes impossible. With durable records, societies retain the capacity to examine their own conduct and correct their course. PRAS therefore functions as the civilizational memory system required for truth-aligned governance.

ANNEX D

Glossary of Canonical Terms

The Liberation Global Constitution — Version 1.2 -----

Adequate Access

Connectivity sufficient to permit secure communication, retrieval of public records, participation in contest procedures, educational access, work opportunity, and civic authentication as defined by baseline standards established under Article II-A.

Artificial Intelligence (AI)

Computational systems capable of performing analytical, predictive, or decision-support functions using algorithmic models or data-driven processes. Under this Constitution, AI systems function as analytical tools assisting human reasoning and may not exercise autonomous coercive authority over persons.

Audit Panel

An independent oversight body empowered to conduct hostile audits of institutional actions, record compliance, secrecy orders, digital rights compliance, and other constitutional obligations. Audit Panels operate under the procedures defined in Article X and COP-G.

Canonical Identifier (CID)

A permanent identifier uniquely identifying a record within the Public Record Accountability System. Canonical identifiers ensure that records remain traceable across time, technological migration, and distributed mirror systems.

Example format: PRAS-[Jurisdiction]-[Year]-[RecordType]-[Sequence]

Coercion

The use or threat of force, deprivation, exclusion, surveillance-for-access, retaliatory restriction, or administrative disabling to compel conduct, speech, belief, or submission.

Coercive Capture

A condition in which institutions or oversight mechanisms intended to serve public accountability become materially controlled by interested parties through funding dependency, appointment control, procedural sabotage, or infrastructural lock-in.

Contest

A formal challenge to the legality, legitimacy, or evidentiary basis of an institutional action. Contests initiate procedural review under COP-G and enforcement mechanisms under Article X.

Digital Civic Access

The constitutional guarantee that persons possess the technological tools and network access necessary for meaningful participation in a digital society. Digital civic access is protected through the rights defined in Article II and Article II-A.

Dispute Resolution

Panel A constitutionally authorized panel empowered to issue terminal merits rulings in constitutional disputes and enforcement cases under Article X and COP-G.

Distributional Impact Summary

A structured identification of groups materially affected by a policy decision and the likely distribution of burdens and benefits, without itself determining the constitutional validity of the policy.

Evidence Hook

A reproducible reference linking an institutional claim, rule, or decision to supporting evidence such as data records, documents, audit logs, or physical evidence. Evidence hooks allow independent verification of institutional claims.

Fairness Statement

A structured explanation of how a policy decision would be justified under conditions of positional uncertainty.

Federation

A voluntary association of adopting entities cooperating to share governance infrastructure including PRAS systems, dispute resolution procedures, audit resources, and educational frameworks. Federation membership requires compliance with the constitutional floor defined in Article IX.

Key A

The originating-authority authorization role within the Two-Key integrity system governing constitutional signing actions, enforcement orders, PRAS system modifications, and other critical constitutional acts.

Key B

The independent oversight authorization role within the Two-Key integrity system. Key B must be held by a threshold group no weaker than three-of-seven members and operates as a safeguard against unilateral alteration of constitutional records or critical constitutional actions.

Legal Person

A juridical entity such as a corporation, partnership, association, trust, or agency recognized by law. Legal persons may exercise rights only insofar as those rights remain consistent with the constitutional protections of natural persons.

Non-Evasion Rule

The principle that recognition of any synthetic, institutional, corporate, automated, or delegated agency must not erase the responsibility of the human, institutional, corporate, governmental, or deploying actors who designed, funded, commanded, constrained, modified, benefited from, or relied upon the system.

Person

A natural human being possessing inherent dignity and constitutional rights under this Constitution.

Artificial systems, synthetic systems, institutions, and legal persons do not possess equivalent moral sovereignty under this Constitution unless expressly recognized through valid amendment, lawful adoption instrument, or justice-specific threshold process consistent with The Liberation-Aligned Justice System and the non-evasion rule.

Principle of Justifiability

The requirement that laws, policies, and institutional actions be capable of justification under conditions in which the identities, status, and positions of affected persons are unknown.

Public Accountability Panel (PAP)

The primary citizen-facing body responsible for receiving complaints, initiating enforcement triggers, and maintaining the public compliance dashboard under Article X.

Public Noncompliance Flag

A PRAS-designated public notice indicating missed duties, responsible authority, elapsed time, and next escalation threshold under Article X.

Public Record Accountability System (PRAS)

The distributed record infrastructure preserving institutional actions, evidence hooks, and audit trails necessary for constitutional accountability. PRAS functions as the civilizational memory infrastructure of truth-aligned governance.

Earlier drafts of Canon Works may use the phrase “Public Record and Accountability System.” Both phrases refer to the same infrastructure. The controlling name in this edition is Public Record Accountability System.

Record Stewardship Unit (RSU)

The technical body responsible for maintaining PRAS infrastructure, schema standards, archival continuity, and integrity verification. RSU possesses no adjudicative authority.

Redaction Map

A structured record describing withheld information within a document including:

- the withheld element;
- justification category;
- approving authority;
- review schedule; and
- sunset condition.

Redaction maps ensure transparency even where limited secrecy is justified.

Relation Graph

A network structure linking related PRAS records, enabling analysis of relationships between laws, budgets, enforcement actions, audits, and dispute rulings. Relation graphs support systemic transparency and policy analysis.

Security Throttling

A narrow, content-neutral network limitation used solely to mitigate technical threats such as denial-of-service attacks, spam, or malware. Security throttling must be time-bounded, evidence-logged, and contestable.

Terminal Merits Ruling

A final binding adjudication issued by a constitutionally authorized dispute panel following completion of review procedures. Terminal merits rulings carry enforcement authority under Article X.

Two-Key Integrity Protocol

A security mechanism requiring two independent authorizations (Key A and Key B) for critical constitutional actions such as record signing, enforcement orders, or institutional certification. The protocol prevents unilateral alteration of constitutional records.

Closing Note

The definitions contained in this glossary serve to stabilize the interpretive language of The Liberation Global Constitution and its annexes. Where ambiguity arises, these definitions guide interpretation unless superseded by explicit constitutional amendment under Article XI.

Annex E — Foundational Reference and Companion Note

This document, The Liberation Global Constitution, stands as the primary procedural and constitutional operating framework of the formally instituted Liberation Triune.

It is to be read in formal relationship with:

- The Declaration of Liberation from All Falsehood, which serves as the testimonial and existential threshold text;
- The Liberation Codex, which develops the philosophical, ethical, and civilizational framework of Liberation;
- and The Liberation-Aligned Justice System, which serves as the primary justice-architecture companion.

The Constitution is not a substitute for the Declaration, the Codex, or the justice companion. It is the operative constitutional layer through which rights, duties, enforcement, record integrity, and institutional accountability are made executable.

It shall therefore be read not as an isolated constitutional text, but as part of a coherent Liberation-aligned ecosystem ordered toward:

Truth → Fairness → Justice → Peace → Flourishing → Correction

Correction completes the Chain by ensuring that every Canonical Work, institution, procedure, and interpretation remains answerable to evidence across time.

No major Liberation document shall be interpreted in a manner that severs it from the wider architecture of testimony, philosophy, constitutional procedure, and domain-specific implementation.