Dikenocracy
CODE OF PLANETARY SYNERGY

Preamble

Dikenocracy is a form of algorithmic state governance based on the principle of *δίκη* (Dike): justice as an objective and measurable balance between a subject's actions and the system's stability.

Power is not held by people, parties, or elites.

Power is held by the function of justice itself, formalized in the form of:

- Open and immutable algorithms,
- Public metrics and transparent data,
- Automated liability procedures,
- Economic incentives aligned with the public good.

Algorithmic authority within Dikenocracy is normative, not agentive.

Algorithms define binding decision rules and execution constraints, but do not constitute Subjects and do not bear causal or legal responsibility.

All responsibility for the deployment, funding, and effects of algorithmic execution remains fully attributable to the originating Subjects, as defined in DKP-1-IDENTITY-001.

Unlike majority democracy or minority technocracy, Dikenocracy avoids subjective decisions.

The function δίκη is appointed by no one and can never be altered by the will of those in power.

It is:

Derived from predefined axioms, such as:

- The "Golden Rule" (do not cause harm you are not willing to accept yourself);
- Avoidance of unnecessary and non-compensable suffering;
- Maximization of long-term sustainability;
- Preservation of nature as the carrier of life;
- Priority of truth and transparency over ideology and personal interests;

And is constantly calibrated by an open consensus mechanism, where participation is distributed according to competence, reputation, and proven accuracy.

Thus, Dikenocracy represents:

- A **self-regulating political system**, where damage automatically generates liability;
- A **self-auditing economic system**, where a subject's profit is mathematically linked to society's benefit;
- A **self-correcting information system**, where lies are economically unprofitable;
- A **self-sustaining ecological system**, where the exploitation of nature is permitted only within the framework of invisible impact.

For the first time in history, Dikenocracy enables a social order in which:

Justice ceases to be a metaphor — and becomes code.

TIU answers the question "how reality works."

Dikenocracy answers the question "how is a sustainable society even possible in such a reality?"

Global Governance Protocol Specification

PREAMBLE

This Code establishes the algorithmic architecture of civilization. The system's goal is to create conditions under which the economic egoism of subjects and the technological expansion of humanity mathematically and inevitably lead to the growth of general welfare and the preservation of the biosphere.

SECTION I. FINANCIAL PHYSICS

Article 1. Dual-Circuit Economy (The Rocket Stage Model)

1.1. The global economy is divided into two independent circuits: Basic (consumption, resources, land) and Venture (space, fundamental science, AI).

1.2. Law of Dynamic Standard (Mirror Peg): The value of currencies and assets in the Basic circuit of developed nations is rigidly pegged to the 5-year moving average of economic growth in the bottom 20% of countries (Development Quintile).

1.3. Venture Gateway: Capital in the Venture circuit is exempt from the Mirror Peg and taxes, provided the "Open Tech Pledge" is signed — requiring the release of developments to the public domain after 5 years.

1.4. Snap Protocol (Emergency Transparency): In the event of a sharp drop (more than 10% per month) in indicators in any region (war, repression), smoothing is disabled, and the aggressor's quotes in the Basic circuit crash instantly.

Article 2. Law of Conditioned Emission

2.1. Financing from global funds is carried out exclusively through targeted smart contracts.

2.2. Funds are unlocked algorithmically (in tranches) only upon the completion of physically verifiable KPIs (built, cured, educated).

SECTION II. PRODUCTION AND RESOURCES

Article 3. Virtual Factory Principle (Tokenized Value Chain)

3.1. Direct export of raw materials is permitted only if the exporter participates in the value-added chain.

3.2. The resource-exporting country automatically receives equity tokens (shares) in the processing enterprises using this resource, regardless of their geography.

3.3. This guarantees that poor nations receive profits from the final high-tech product without forced localization of factories.

Article 4. Law of Technological Inheritance

4.1. Any technology necessary for life support or created within the preferential Venture circuit enters the Public Domain 5 years after patent registration.

SECTION III. HUMAN CAPITAL

Article 5. Global Qualification

5.1. A single planetary standard of competence is introduced. Diplomas are confirmed by passing a standardized AI exam and are recognized in all jurisdictions.

Article 6. Human Capital Lease Protocol

6.1. Right to Exit: Citizens have the absolute right to leave any jurisdiction. Relocation costs from depressed zones are covered by a global fund.

6.2. Talent Leasing: Upon the relocation of a specialist, the recipient country pays an annual commission (Lease Fee) to the donor country.

6.3. Post-Factum Principle: Payment is made only after a year of successful work by the specialist, preventing the creation of "fake diploma factories."

6.4. Educational DAO: Lease funds do not go to the government budget but to a transparent Education Fund in the region of origin.

SECTION IV. SECURITY AND LIABILITY

Article 7. Peace Staking

7.1. To access the Global Trade Network, a state deposits a pledge (Stake) into an Escrow smart contract. The stake size is proportional to GDP.

7.2. As long as the state maintains peace, dividends from global GDP growth accrue on the stake.

7.3. In the event of aggression, the stake is automatically burned (Slashing).

Article 8. The Kill Switch Law

8.1. In the event of military aggression recorded by independent monitoring, or upon exhaustion of the Peace Stake, the violating region is automatically disconnected from the global financial, energy, and logistical infrastructure.

8.2. The use of weapons entails the write-off of the aggressor's assets in an amount 10 times the damage caused.

SECTION V. POLITICAL MECHANICS

Article 9. Managerial Governance

9.1. The institution of irremovable power is abolished. Territories are managed by Regional Operators.

9.2. An Operator is hired for the duration of a specific KPI. Failure to meet the KPI leads to automatic contract termination.

Article 10. Glass Pocket Law

10.1. All state/regional budget transactions are displayed on a public blockchain in real-time. Secret expenditure items are prohibited.

Article 11. Ban on Lobbying

11.1. Any covert interaction of private capital with legislative algorithms or operators is a criminal offense.

SECTION VI. BIOSPHERE BALANCE

Article 12. Full Product Cost

12.1. The cost of full disposal and environmental damage restoration is algorithmically included in the price of any good.

Article 13. Guardian Status and Invisible Extraction

13.1. 40% of land is declared a Biosphere Reserve.

13.2. Invisible Extraction: Resource extraction in reserves is permitted exclusively by methods that do not disturb the surface layer integrity (robotized tunnels, bio-leaching). Open pits and logging are prohibited.

13.3. Residents of reserves receive the status of Biosphere Operators. Their income is generated by a smart contract based on sensor data (biomass index, CO2 levels, biodiversity).

SECTION VII. INFORMATION HYGIENE

Article 14. Decentralized Verification (Proof-of-Truth)

14.1. Public statements by officials are verified by a decentralized network of validators.

14.2. Quadratic Protection: The cost of buying validator votes grows exponentially (Cost = Votes²), making a capital attack economically impossible.

14.3. Competence Weight: A validator's vote is weighted by their reputation in a specific field of knowledge (EigenTrust algorithm).

Article 15. Open Algorithms

15.1. The source code of all algorithms influencing resource allocation, social rating, or news feeds must be Open Source.

SECTION VIII. SOCIAL JUSTICE

Article 16. Progressive Inheritance Tax

16.1. Personal assets are heritable. Infrastructure capital and power are not subject to inheritance. Ultra-large fortunes return to the Global Development Fund after the owner's death.

Article 17. Unconditional Basic Resource (UBR)

17.1. Every human is guaranteed a minimum set of resources for survival (food, shelter, connectivity) by right of birth.

Article 18. Social Contribution

18.1. Receipt of UBR imposes an obligation to participate in education, creativity, or socially useful activity. Total passivity leads to a reduced rating for access to additional benefits.

Appendix A

Technical Implementation and Mitigation of All Critical Vulnerabilities

A.1. The Main Equation of Civilization Motion (Immutable since 2025)

At any moment in time t, the Network must maintain:

$dW/dt \geq k \cdot E(t) \cdot T(t) \cdot B(t)^{2.83}$

Where:

- $W(t)$ — Global welfare + biosphere health (in arbitrary utility units)
- $E(t)$ — Total egoistic activity of all agents
- $T(t)$ — Rate of technological expansion (logarithm of available energy and compute)
- $B(t)$ — Biosphere Health Index (0...1, measured by Physical Truth Layer)
- k = 0.94...1.06 (calibrated every 3 years by independent audit)
- α = 2.83 — Measured fractal dimension of global ecosystems (NASA EarthData 2000–2025)
- $B_{\min}=0.68-Hard threshold; if \$B(t)<B_{\min}\$,$ all Kill Switches activate simultaneously.

A.1a Parameter Governance Invariant

> All coefficients, bounds, and calibration parameters of the Main Equation SHALL NOT be optimized, tuned, or adjusted on-chain or through continuous execution.
>
> Any modification of these parameters MUST be performed exclusively via DKP-4-UPGRADE-001 and SHALL require prior validation under DKP-8-SIMULATION-001.
>
> No operational, financial, crisis, or enforcement protocol MAY directly or indirectly modify Equation parameters.

Violation for more than 180 consecutive days = System Failure $\rightarrow$ Temporary manual control by the consortium of the first six nodes.

A.2. Solving the Oracle Problem: Physical Truth Layer (Four-Layer Stack)

All data upon which Code smart contracts depend is accepted only through the following stack:

Level 0 — Space (Weight 65–75%)

- Constant monitoring of 100% land and ocean via SAR satellites + hyperspectral cameras.
- $\geq$ 28,000 LEO satellites by 2030.
- Raw cryptographic signing of data on board + zk-proof upload (Starling Lab + SpaceKnow + ESA open-source stack).

Level 1 — Autonomous Drones and Ground Sensors (Weight 15–25%)

- Geohashed 4K video + thermal imaging + LiDAR with RTK-GPS (± 2 cm).
- Hash and signature uploaded before drone return (Zipline/Rwanda, Wing/Alphabet).

Level 2 — Decentralized Human Validators (Weight $\leq$ 10%)

- Quadratic funding + EigenTrust reputation.
- Stake for lying: $10–100M (Kleros + UMA).

Level 3 — Oracle of Oracles

- Bayesian ensemble of all levels. Divergence > 7% $\rightarrow$ automatic arbitration with a $500M stake. All related tranches are frozen until resolution (max 14 days).

A.3. Protection Against External Military Pressure (Pre-Bootstrap Shield)

Until the network reaches 18% of World GDP ($\approx$2031–2032):

3.1. Critical nodes are physically distributed across at least 5 different geopolitical blocks possessing nuclear weapons or their equivalent.

3.2. Each node must have a fully autonomous energy source $\geq$ 800 MWh/year of one of the following types (by priority):

1. Ultra-deep geothermal station ($\geq$15 km, Quaise/Fervo/Kenya Rift-2).
2. SMR Gen-IV (NuScale, BWRX-300, RITM-200N, etc.) with open safety code and fuel in an IAEA bank.
3. Closed hydrogen-bromine cycle + orbital microwave energy (Virtus Solis/Reflect Orbital).
4. Any combination of the above.
   Status confirmed by Physical Truth Layer Levels 0–1.

3.3. Dead Man Switch:

Upon physical seizure or destruction of any node, $\geq$ 50% of all Peace Stakes globally are automatically burned and distributed to the remaining nodes. Attacking the network becomes economic suicide.

A.4. Mercy and Force Majeure (Compassion Clause)

The Snap Protocol and all Kill Switches are automatically suspended for 180 days in the event of:

- Eruption > VEI-6
- Asteroid > 200 m
- Pandemic with lethality > 15%
- Confirmed drop in B(t) due to natural, non-anthropogenic reasons (verified by Physical Truth Layer).

Control transfers to the "Council of Crisis Mercy" (9 people, sortition from 1000 scientists with EigenTrust > 0.97).

All Mercy actions, suspensions, and discretionary decisions SHALL operate strictly within the boundaries defined by DKP-7-SCOPE-001.

Mercy SHALL NOT:

- expand system applicability,
- override S2 or S3 domain prohibitions,
- create new rights, authorities, or governance powers,
- persist beyond explicitly declared Crisis Scope.

Mercy modifies response severity only. It SHALL NOT extend jurisdiction or normative authority.

A.5. Minimum Startup Cluster (6+1)

The Network is considered irreversibly launched upon simultaneous online status of:

1. Zanzibar
2. Prospera / Roatán
3. NEOM-2 or any SAR of Saudi Arabia
4. Abu Dhabi Global Tech Zone
5. Tallinn + Tartu (Estonia 2.0)
6. Kigali + Bugesera Tech City
- One "Wild" Node (any entity that fully implements the Code + Appendix A within $\leq$ 24 months).

After this, new territories connect only via a referendum of 67% of the adult population + deposit of a Peace Stake.

A.6. Ban on Inherited Control over Critical Oracle Infrastructure

No natural or legal person may own (directly or indirectly) more than:

- 0.7% of Level 0 satellites
- 2% of geothermal wells or power units of critical nodes

Violation = instant burning of all violator's stakes + 20-year ban on network participation.

Closing Provision

This Appendix A is an integral part of the Code of Planetary Synergy and holds supreme legal force over any national laws in participating jurisdictions.

We no longer ask the old world for permission.

We are building a new one beside it — faster, cleaner, and so much more profitable that remaining outside will become economic suicide.

Signed with irreversible digital signatures of the six startup nodes

December 10, 2025.

Genesis Block #0 (Technical Specification)

JSON


```
{
  "block_height": 0,
  "timestamp": "2025-12-10T23:59:59.000Z",
  "previous_hash":
"0x0000000000000000000000000000000000000000000000000000000000000000",
  "consensus_protocol": "Proof-of-Synergy v1.0 (Physical Truth Layer + Peace Staking)",
  "difficulty_target": "0x00000fffffffffffffffffffffffffffffffffffffffffffffffffffffffffff",
  "nonce": 0,
  "initial_parameters": {
    "k": 1.000000000000000,
    "alpha": 2.83,
    "B_min": 0.68,
    "B_current_at_genesis": 0.7104
  },
  "physical_anchors": {
    "mauna_loa_co2_ppm": 426.91,                    // NOAA measurement, Dec 10, 2025
    "global_temperature_anomaly_C": "+1.48",        // Copernicus ECMWF, Dec 2025
    "living_planet_index_2024_baseline": 0.312,     // WWF/ZSL 2024 -> converted to B(t)
    "planetary_boundaries_safe_space_violated": "6/9",    // Stockholm Resilience Centre status
    "hash_of_codex_v1.3_plus_appendix_A":
"sha256:9f2a7c8e1d4b6f91a3e8c7d5b9f0e1a2c4d6e8f0a1b2c3d4e5f60718293a4b5c"
  },
  "immutable_message": "We do not ask the dying world for permission. We build the next one
beside it, faster and cleaner. Let the Equation run forever.",
  "signatories": [
    "zanzibar_node_01_ed25519:0xA7f3...",
    "prospera_node_01_ed25519:0xB9e1...",
    "neom_node_01_ed25519:0xC4d2...",
    "abudhabi_node_01_ed25519:0xF1a9...",
    "tallinn_node_01_ed25519:0xE6c7...",
    "kigali_node_01_ed25519:0xD8b4...",
    "wild_node_alpha_ed25519:0x????..."         // Reserved for the first decentralized sovereign node
  ],
  "merkle_root_of_first_six_peace_stakes": "0x7e9f4a1b..."
}
```

Explanatory Note to Parameters (Annotation)

1. Physical Anchors

- **CO2 = 426.91 ppm:** Value recorded at the moment of launch. Serves as the "Tombstone" of the old climatic epoch.
- **B_current = 0.7104:** Current Biosphere State Index. Leaves a buffer of only 0.0304 before the critical threshold ($B_{min} = 0.68$). This is a mathematical expression of remaining time (estimated 14–18 years at current trends).
- **6/9 Planetary Boundaries:** Fixation of the historical fact of the violation of 6 out of 9 planetary boundaries of sustainability.

2. Cryptographic Signature (Signatories)

- **Wild Node Alpha:** The signature slot is intentionally left empty (`0x????...`). This is an open vacancy for the first independent jurisdiction or city-state to fully implement the Code without prior agreements, confirming the decentralized nature of the network.

3. Immutable Message

- The text of the manifesto is embedded in the Genesis Block forever, declaring the refusal to attempt to "fix" the old system in favor of building a new parallel reality based on physical laws (TIU).

Glossary & Definitions

- **Genesis Block:** The primary data block in the chain (Block Height 0), having no predecessor. It rigidly fixes the system's initial parameters, physical constants, and the planet's state at the moment of launch. It serves as an immutable reference point for the entire subsequent transaction history.
- **Proof-of-Synergy (PoS):** A consensus protocol replacing traditional Proof-of-Work and Proof-of-Stake. Block validation occurs not through burning electricity or accumulating capital, but based on proven contribution to reducing system entropy (biosphere restoration, social stability, technological efficiency).
- **Physical Truth Layer:** The layer of objective truth. A network of verified hardware oracles (satellites, sensors, IoT) that transmit data about the physical world's state (temperature, CO2, sea level) directly to the blockchain. This makes falsification of environmental or industrial reports impossible.
- **B (Biosphere Integrity Index):** A dynamic calculated index (from 0 to 1) reflecting the planetary system's ability to support life.
    - $B_{current}$: Current value.
    - B_{min} *(0.68)*: Critical threshold (point of no return), below which irreversible cascading ecosystem collapse begins.

- **Peace Staking:** An economic collateral mechanism where assets are "frozen" not for passive income, but as a guarantee of non-aggression and Code compliance. In case of violation (aggression or ecocide), the stake is automatically burned or redistributed to repair damage.
- **Wild Node:** A network node launched by an independent party (city, corporation, or community) without prior coordination with the founders, but in full compliance with the protocol. The presence of "Wild Nodes" confirms the system's decentralization and viability outside its creators' control.
- **The Equation:** A fundamental mathematical model (based on the Theory of the Informational Universe - TIU) describing the balance between information, energy, and entropy. In the Code's context, "Let the Equation run" means making decisions based on mathematical survival optimization rather than political will.
- **Immutable Message:** A text message cryptographically embedded in the Genesis Block code. It is the philosophical manifesto and "constitution" of the system, which is technically impossible to delete or edit as long as the network exists.

DKP-0-ORACLE-001

Physical Truth Layer Protocol (PTL)

Version: 1.1
Status: Architecture Lock Candidate
Layer: L0
Anchored to: Genesis Block #0 (2025-12-10)

---

1. Purpose

The Physical Truth Layer (PTL) defines the **sole admissible interface between physical reality and the Dikenocracy governance system**.

Its function is to produce a **bounded, physically grounded, cryptographically verifiable representation of observable reality**, independent of political, economic, or human discretion.

The PTL produces **physical state only**.

The PTL does not:

- interpret meaning,

- infer intent,
- assign value,
- perform policy reasoning,
- infer subjective or semantic states.

---

2. System Position and Anchoring

This protocol is an integral extension of Appendix A.2 of the Code of Planetary Synergy and is anchored to **Genesis Block #0 (2025-12-10)**.

Compatibility with Genesis Block physical anchors and parameters is a **mandatory validity condition** for any PTL implementation.

PTL outputs are **non-normative** and may only be consumed by higher layers under explicitly defined activation and scope rules.

---

3. Scope

This protocol governs:

- oracle admissibility,
- data ingestion constraints,
- oracle weighting and ownership caps,
- temporal validity of data (TTL),
- data aggregation methodology,
- divergence detection and arbitration,
- production of raw physical indices required by higher layers.

This protocol explicitly excludes:

- human testimony or manual input,
- semantic interpretation,
- intent inference,
- subjective state attribution,
- policy reasoning,
- cross-layer feedback or parameter adjustment.

---

4. Core Definitions

4.1 Physical State Vector S(t)

A time-indexed vector of **physically measurable variables**, derived exclusively from admissible oracle inputs.

4.2 Oracle Source

A hardware-bound system producing **cryptographically signed physical measurements**, traceable to a registered oracle identity.

4.3 Oracle Owner

A natural or legal person controlling one or more oracle sources.

4.4 Confidence Weight w_i

A normalized reliability contribution of an oracle source, bounded and capped by protocol constraints.

4.5 Coverage

The fraction of the target physical domain that is actively observed by valid oracle sources with non-zero confidence.

4.6 Data Staleness (TTL)

The maximum admissible age of a datum before its confidence weight is **forced to zero**.

4.7 Independent Oracle Classes

Distinct measurement modalities defined by **physical separation of sensing mechanisms**.

4.8 Divergence Event

A statistically significant disagreement between posterior distributions produced by **independent oracle classes**.

---

5. Measurement Classification (Mandatory)

All PTL outputs MUST be explicitly classified as one of the following:

5.1 Direct Physical Measurements

Directly observable quantities requiring no semantic interpretation.

Examples include: position, speed, acceleration, mass, temperature, radiation, pressure, noise level, duration, exposure.

5.2 Proxy-Based Measurements

Derived indicators correlating with physical processes but **not equivalent to subjective, semantic, or normative states**.

Examples include: load indices, stress proxies, fatigue indicators, environmental risk proxies.

Proxy-based outputs MUST:

- explicitly declare the proxy model used,
- include propagated uncertainty,
- explicitly state that the result is not a subjective state.

5.3 Non-Measurable Domains (Explicitly Excluded)

The PTL SHALL NOT emit outputs concerning:

- intent,
- dignity,
- belief,
- responsibility,
- consent,
- moral, cultural, or social harm.

---

6. Independent Oracle Classes

The PTL defines the following independent oracle classes:

- Orbital (satellite-based remote sensing),
- Ground (fixed terrestrial or marine sensors),
- Autonomous (mobile or robotic sensing platforms).

Divergence detection applies **exclusively across classes**, not within a single class.

---

7. Data Ingestion Rules

All data MUST:

- be cryptographically signed at the source,
- be time-stamped with a verifiable clock,
- be traceable to a registered oracle identity,
- be delivered in an open, publicly decodable schema.

Proprietary or non-decodable data formats SHALL be rejected regardless of signature validity.

Zero-knowledge proofs MAY be used to verify authenticity without revealing proprietary sensor internals.

No data may be modified, normalized, aggregated, or interpreted at ingestion time.

---

8. Oracle Weighting and Anti-Collusion Constraints

- Maximum confidence weight per oracle source: **4%**
- Maximum combined confidence weight per oracle owner: **4%**

Ownership caps apply regardless of the number or distribution of devices.

Exceeding caps results in:

- automatic zeroing of excess weight,
- slashing of the violating owner’s remaining stake, where applicable.

---

9. Temporal Validity and Data Staleness

All data types SHALL have an explicit TTL.

Data exceeding its TTL SHALL have its confidence weight set to zero.

Stale data MUST NOT be:

- extrapolated,
- interpolated,
- substituted,
- averaged into current state.

Oracle silence, loss of signal, or zero-weight conditions:

- SHALL NOT be interpreted as neutral or zero-impact physical states,
- MUST propagate upward as **explicit uncertainty, degradation, or halt signals**.

---

10. Data Aggregation Method

The PTL aggregates admissible data using a **deterministic Bayesian ensemble**.

- Oracle inputs act as likelihood updates, not votes.
- Prior weights reflect long-term reliability.
- Posterior distributions define S(t).

Given identical inputs, aggregation MUST be reproducible.

All aggregation pipelines MUST be auditable and explainable.

---

11. Divergence Detection and Arbitration

A Divergence Event is triggered when posterior distributions across independent oracle classes differ by more than **7%**.

Upon a Divergence Event:

- a divergence flag is emitted,

- all dependent state-based transactions SHALL be frozen.

Maximum arbitration window: **14 days**.

Resolution requires:

- convergence within the threshold, or
- exclusion of faulty or compromised sources.

---

12. Outputs

The PTL produces the following immutable outputs:

- Signed Physical State Vector S(t)
- Oracle confidence weights
- Coverage metrics
- Divergence flags
- Confidence envelope for each output $\in [0,1]$
- Raw Biosphere Integrity Index B(t)

B(t) is a **composite physical index**, constructed exclusively from PTL-admissible measurements.

The **model, aggregation logic, weighting, and calibration of B(t)** are **not defined in PTL** and MUST be explicitly specified in **DKP-8-SIMULATION-001**.

PTL SHALL NOT modify, tune, normalize, or reinterpret B(t) beyond emitting its raw, model-declared output.

Until an attached and valid L8 calibration bundle exists, B(t) SHALL be treated as **informational only** and SHALL NOT trigger enforcement.

---

13. Systemic Halt Conditions

All dependent governance execution layers MUST halt if any of the following conditions occur:

- aggregate confidence falls below **60%**,
- global coverage falls below the minimum operational threshold,
- systemic oracle integrity is compromised.

Systemic Halt:

- blocks execution of L2 and higher layers,
- SHALL NOT erase, reset, reinterpret, or invalidate L1 state,
- preserves identity attribution, impact records, and subject continuity.

---

14. Crisis Mercy Exception

If a Crisis Mercy status is formally activated under Appendix A.4 of the Code of Planetary Synergy, and the PTL confirms that oracle degradation is caused by **non-anthropogenic global physical events**, enforcement of Systemic Halt MAY be temporarily deferred.

For avoidance of doubt:

Events resulting from **human action, negligence, sabotage, coordinated sensor manipulation, or deliberate oracle interference** SHALL NOT be classified as non-anthropogenic.

Such deferral:

- DOES NOT modify TTL values,
- DOES NOT restore stale data weights,
- DOES NOT alter aggregation logic,
- IS strictly time-limited in accordance with Appendix A.4,
- DOES NOT create normative or precedential authority (see DKP-7-SCOPE-001).

---

15. Cross-Layer Isolation Invariant

No higher-layer protocol may:

- influence oracle weights,
- modify TTL values,
- alter aggregation logic,
- suppress divergence flags,
- reinterpret confidence envelopes.

Violation constitutes a **critical system integrity breach**.

---

16. Table of Constants

Parameter	Value
Max oracle source weight	4%
Max oracle owner weight	4%
Divergence threshold	7%
Arbitration window	14 days
Systemic confidence halt	< 60%
Minimum global coverage	80%

---

17. TTL Registry (Normative)

Data Type	Maximum TTL
Atmospheric CO_2 concentration	1 hour
Surface temperature (land/sea)	24 hours
Active fire detection	10 minutes
Biodiversity indices	30 days
Land-use change	7 days

---

18. Non-Override and Finality

This protocol is immutable once deployed.

Any modification requires:

- a new protocol identifier,
- an explicit incompatibility declaration,
- re-anchoring assessment against Genesis Block #0.

DKP-0-TIME-001

Dikenocratic Time & Date Index Protocol (DTI)

Version: 1.0

---

1. Purpose

DKP-0-TIME-001 defines a **non-religious, event-neutral, deterministic system for counting days and years** within the Dikenocracy framework.

The protocol establishes:

- a canonical **absolute civil day index**,
- a **fixed-length governance year** for accountability and reporting,
- precise and auditable **conversion rules** to and from the Gregorian calendar when external interoperability is required.

This protocol explicitly avoids:

- religious eras or holidays,
- historical or mythological reference events,
- variable or exception-based calendar logic.

---

2. Design Principles

1. **Neutrality**
   Time MUST NOT be anchored to religious, cultural, political, or personal events.

2. **Determinism**
   Any date MUST be uniquely computable from its canonical representation.

3. **Auditability**
   Any record MUST allow independent recomputation of its time index.

4. **Governance Fitness**
   Time units MUST be simple, fixed-length, and suitable for legal, financial, and KPI logic.

5. **Interoperability**
   Explicit conversion rules to and from civil calendars MUST be provided.

---

3. Definitions

- **JDN (Julian Day Number)**
  An integer count of civil days (midnight-to-midnight) in the proleptic Gregorian calendar.

DTI-Day
The canonical absolute civil day index used by Dikenocracy.
Definition:

```
DTI-Day = JDN
```

-
- **DTI-Year (DY)**
  A governance year consisting of exactly **360 consecutive DTI-Days**.

- **Day-of-Year (DOY)**
  A 1-based index of a day within a DTI-Year, in the range **1…360**.

---

4. Normative Time Units

4.1 Base Unit

- The base temporal unit of DKP-TIME-001 MUST be the **civil day**.

- Sub-day units (hours, minutes, seconds) MUST NOT be required by this protocol.

4.2 Governance Year

- A DTI-Year MUST contain exactly **360 DTI-Days**.
- Leap days, leap years, or corrective rules MUST NOT exist.
- Year boundaries MUST be defined purely arithmetically.

---

5. Canonical Date Representation

5.1 Numeric Form

Given a canonical `DTI-Day`:

```
DY  = floor(DTI-Day / 360)
DOY = (DTI-Day mod 360) + 1
```

5.2 String Form

```
DY<dy>-<doy>
```

Where:

- `<dy>` is a signed integer year index,
- `<doy>` is a zero-padded three-digit day index (001–360).

Example:

```
DY6836-084
```

---

6. Conversion Rules (Normative)

6.1 Gregorian → Dikenocratic

Given a Gregorian civil date `(year, month, day)`:

1. Compute the **JDN** using a standard astronomical algorithm.
2. Set `DTI-Day = JDN`.
3. Compute `(DY, DOY)` using Section 5.

6.2 Dikenocratic → Gregorian

Given `(DY, DOY)`:

1. Validate `DOY ∈ [1, 360]`.

Compute:

```
DTI-Day = DY × 360 + (DOY - 1)
```

2.
3. Convert `DTI-Day (JDN)` to Gregorian `(year, month, day)`.

6.3 Validation

- Invalid `DOY` values MUST be rejected.
- `DY` MAY be negative.
- Derived fields MUST NOT override `DTI-Day`.

---

7. Interoperability

- Gregorian dates MAY be shown for human readability.
- Any authoritative record MUST include:
    - `DTI-Day`, or
    - canonical `(DY, DOY)`.

- In case of conflict, **DTI-Day is authoritative**.

---

8. Storage, Signing, and Audit

- Signed records SHOULD store:
    - `DTI-Day` (authoritative),
    - optionally `(DY, DOY)` as derived fields.
- Audits and dispute resolution MUST reference `DTI-Day`.

---

9. Normative Test Vectors

Implementations MUST reproduce these values exactly.

Gregorian Date	JDN (DTI-Day)	DY	DOY	Canonical
2026-01-01	2461042	6836	83	DY6836-083
2026-01-02	2461043	6836	84	DY6836-084
1970-01-01	2440588	6779	149	DY6779-149
2000-01-01	2451545	6815	26	DY6815-026

Failure to match these vectors constitutes a protocol violation.

---

10. Reference Implementation (Canonical)

```
from __future__ import annotations
from dataclasses import dataclass

# Gregorian <-> JDN (Fliegel–Van Flandern)
```

```
def gregorian_to_jdn(year: int, month: int, day: int) -> int:
    a = (14 - month) // 12
    y = year + 4800 - a
    m = month + 12 * a - 3
    return (
        day
        + (153 * m + 2) // 5
        + 365 * y
        + y // 4
        - y // 100
        + y // 400
        - 32045
    )

def jdn_to_gregorian(jdn: int) -> tuple[int, int, int]:
    a = jdn + 32044
    b = (4 * a + 3) // 146097
    c = a - (146097 * b) // 4
    d = (4 * c + 3) // 1461
    e = c - (1461 * d) // 4
    m = (5 * e + 2) // 153
    day = e - (153 * m + 2) // 5 + 1
    month = m + 3 - 12 * (m // 10)
    year = 100 * b + d - 4800 + (m // 10)
    return year, month, day

DTI_YEAR_LENGTH = 360

@dataclass(frozen=True)
class DikenocraticDate:
    dy: int
    doy: int
    def __post_init__(self):
        if not (1 <= self.doy <= DTI_YEAR_LENGTH):
            raise ValueError("DOY must be in 1..360")
    def canonical(self) -> str:
        return f"DY{self.dy}-{self.doy:03d}"
```

```
def jdn_to_dikenocratic(jdn: int) -> DikenocraticDate:
    return DikenocraticDate(jdn // 360, (jdn % 360) + 1)

def dikenocratic_to_jdn(dd: DikenocraticDate) -> int:
    return dd.dy * 360 + (dd.doy - 1)

def gregorian_to_dikenocratic(y: int, m: int, d: int) ->
DikenocraticDate:
    return jdn_to_dikenocratic(gregorian_to_jdn(y, m, d))

def dikenocratic_to_gregorian(dy: int, doy: int) -> tuple[int, int,
int]:
    return jdn_to_gregorian(dikenocratic_to_jdn(DikenocraticDate(dy,
doy)))
```

---

11. Rationale (Non-Normative)

Time in Dikenocracy is treated as an **operational index**, not as a cultural narrative.
`DTI-Day` provides a continuous, neutral axis.
`DTI-Year` provides a stable governance cycle.

DKP-1-AXIOMS-001

Axioms Protocol
Version 1.0

---

1. Purpose

The Axioms Protocol defines the non-negotiable boundary conditions of the Dikenocracy system.

Axioms are not moral statements and not policy goals. They are invariant constraints that bound all measurement, optimization, and enforcement logic.

No higher-layer protocol may violate an axiom, regardless of calculated benefit.

---

2. System Position and Anchoring

This protocol operates above the Physical Truth Layer (DKP-0-ORACLE-001) and below all impact, justice, and economic protocols.

This protocol is anchored to the predefined axioms stated in the Preamble of the Code of Planetary Synergy and is bound to Genesis Block #0 (2025-12-10).

Any interpretation or implementation of this protocol MUST remain compatible with the immutable civilizational motion equation defined therein.

Axioms do not process data. They constrain how data-derived metrics may be interpreted and acted upon.

---

3. Axiom Structure

Each axiom is defined as:

- a forbidden state, or
- a hard priority ordering between competing system objectives.

Axioms are evaluated as constraints, not as terms in an optimization function.

---

4. Core Axioms

Axiom A1 — Preservation of Life

System actions MUST NOT knowingly increase irreversible loss of human life **or biospheric life** beyond the minimum required to prevent greater systemic collapse.

The definition of such minimum required conditions is exclusively governed by DKP-4-CRISIS and SHALL NOT be inferred, approximated, or declared by operational, economic, or enforcement protocols.

Life preservation has absolute priority over economic growth, efficiency, or political stability.

Interpretation Constraint:
The determination of “minimum required conditions”
SHALL NOT be inferred by operational or economic protocols
and SHALL be constrained by DKP-7-SCOPE-001.

Axiom A1a — Risk Symmetry and Voluntary Lethal Risk

1. No subject may be compelled to participate in armed violence or in activities involving lethal risk on behalf of the system.

2. Any subject has the right to refuse military service or combat participation on any grounds, including religious, ethical, or pacifist convictions.

3. The system SHALL preserve risk symmetry: a subject who does not participate in verified collective security risk SHALL NOT receive benefits, subsidies, or priority access derived directly from such risk.

4. Risk symmetry SHALL be enforced through access rules and compensation logic, not through punishment, stigma, or coercion.

5. Refusal to assume lethal risk SHALL NOT constitute a violation, disloyalty, or fault within the system.

Axiom A2 — Systemic Sustainability

System actions MUST NOT degrade long-term system viability in exchange for short-term gains.

Any action that results in sustained degradation of biospheric integrity, as reflected in Physical Truth Layer outputs (including B(t)), constitutes a violation of this axiom.

Actions that improve short-term metrics at the cost of long-term collapse are forbidden.

Axiom A3 — Physical Reality Supremacy

System decisions MUST be grounded in Physical Truth Layer outputs.

Narratives, beliefs, intentions, or declared goals SHALL NOT override measured physical reality.

Axiom A4 — Irreversibility Aversion

System actions SHOULD minimize irreversible damage when reversible alternatives exist.

Irreversible transitions require demonstrable necessity verified by irreversible impact models under DKP-1-IMPACT.

Axiom A5 — Externality Accountability

Actions that shift harm outside the measured system boundary are forbidden unless the externality is explicitly measured and bounded.

Unmeasured externalization is treated as maximum-impact damage.

The full cost of environmental and systemic externalities SHALL be included in the effective cost of any action or product, in accordance with Article 12 of the Code of Planetary Synergy (Full Product Cost).

Axiom A6 — Truth Priority

Suppression, distortion, or strategic withholding of physically verifiable truth is forbidden when it materially affects system stability.

Truth is treated as a structural requirement, not a moral virtue.

Axiom A7 — Minimum Suffering Constraint

Among actions that satisfy all higher-priority axioms and are indistinguishable with respect to them, the system SHALL apply a non-amplification constraint on suffering.

Suffering is treated as a measurable state variable of subjects, quantified via physical proxies derived from the Physical State Vector S(t), and SHALL NOT be treated as an ethical objective or optimization target.

Suffering is evaluated solely to prevent unnecessary additional suffering between otherwise admissible and axiomatically equivalent actions.

Suffering SHALL NOT be optimized, minimized globally, or traded against other system objectives, and SHALL NOT serve as a primary decision criterion.

---

5. Axiom Evaluation Rules

1. Axioms are evaluated before any optimization or scoring.
2. Violation of any axiom invalidates an action regardless of utility score and propagates to higher-layer protocols for enforcement.
3. Axioms are not additive and cannot be traded off against each other.
4. Conflicts between axioms are resolved only by higher-priority axioms.

---

6. Priority Ordering

The priority order of axioms is fixed and non-negotiable.

Priority Ordering Table

Priority	Axiom ID	Description
1	A1	Preservation of Life
2	A2	Systemic Sustainability
3	A3	Physical Reality Supremacy
4	A4	Irreversibility Aversion
5	A5	Externality Accountability
6	A6	Truth Priority
7	A7	Minimum Suffering Constraint

Lower-priority axioms SHALL NOT override higher-priority ones.

---

7. Prohibited Interpretations

The following interpretations are explicitly forbidden:

- Treating axioms as optimization goals
- Encoding axioms as weighted utility terms

- Temporarily suspending axioms for efficiency
- Overriding axioms by human discretion
- Reinterpreting axioms based on political, cultural, or situational context

---

8. Invariance and Finality

Axioms are invariant once deployed.

Any modification requires:

- a new protocol identifier
- explicit declaration of incompatibility
- full-system revalidation under DKP-8-SIMULATION
- ratification by no less than **67% of active validating nodes**, as defined in Appendix A.5 of the Code of Planetary Synergy

DKP-1-IDENTITY-001

Identity & Subject Protocol

Version 1.0

---

1. Purpose

The Identity & Subject Protocol defines what constitutes a **Subject** within the Dikenocracy system and how actions, effects, and responsibility are causally bound to that Subject across time, delegation layers, and system boundaries.

This protocol establishes **attribution**, not punishment.
It performs **identity binding and responsibility linkage only**.

This protocol does **not**:

- measure impact magnitude,

- calculate justice,
- assign sanctions or compensation,
- interpret intent, motive, or moral value.

---

2. System Position

This protocol operates:

- above DKP-0-ORACLE-001 (Physical Truth Layer),
- alongside DKP-1-IMPACT-001 (Impact Measurement Protocol),
- below DKP-1-JUSTICE-001 (Justice Function Protocol),
- prior to all economic, governance, security, and enforcement protocols.

All attribution performed by this protocol MUST rely exclusively on outputs produced by DKP-1-IMPACT-001.

---

3. Core Definitions

3.1 Subject

A **Subject** is any entity capable of initiating, amplifying, sustaining, or failing to prevent a state transition that is measurable under DKP-1-IMPACT-001.

Subjects include, but are not limited to:

- individual humans,
- legal entities,
- collective groups,
- decentralized organizations (e.g., DAOs),

- automated or algorithmic systems,
- artificial intelligences,
- hybrid human–machine assemblies.

Subject status is **functional**, not moral or legal.

3.2 Action

An **Action** is any intervention, omission, or sustained process attributable to a Subject that produces a measurable change in the Physical State Vector S(t).

Failure to act SHALL be treated as an Action when omission contributes causally to measurable impact.

3.3 Responsibility

Responsibility is the persistence of causal linkage between a Subject and measurable impacts arising from its actions or omissions, independent of intent, awareness, foresight, or justification.

---

4. Identity Binding Invariant

For every detected impact vector I_i produced by DKP-1-IMPACT-001:

- at least one Subject SHALL be causally attributable,
- attribution MUST be traceable through an auditable causal chain,
- absence of intent, prediction, or awareness SHALL NOT invalidate attribution.

Unattributed or untraceable impacts constitute a critical system violation.

---

5. Delegation and Automation

Delegation transfers **execution**, not responsibility.

Where a Subject:

- delegates action to another Subject,
- deploys automated or algorithmic systems,
- operates through intermediaries, platforms, or agents,

the originating Subject SHALL retain causal responsibility unless an explicit, auditable counter-binding is recorded and validated.

Artificial intelligences and automated systems SHALL be treated as Subjects for attribution purposes but SHALL NOT acquire exemption, immunity, or sovereignty.

Smart contracts, autonomous agents, scripts, and algorithmic execution mechanisms SHALL NOT be considered independent Subjects under any circumstances.

Such mechanisms operate exclusively as proxy-subjects, executing delegated intent or predefined logic on behalf of an originating Subject.

All actions performed by smart contracts or automated agents SHALL be causally and legally attributed to the originating Subject(s) who deployed, authorized, funded, or materially benefited from their execution, unless an explicit, auditable counter-binding assigns responsibility to another identifiable Subject.

---

6. Collective and Distributed Subjects

Where actions arise from coordinated, collective, or emergent behavior:

- responsibility MAY be distributed across multiple Subjects,
- distribution SHALL be proportional to measurable causal contribution,
- collective attribution SHALL NOT erase individual responsibility.

Temporary coalitions, swarms, and decentralized collectives constitute valid Subjects for the duration of their active coordination.

---

7. Temporal Persistence of Identity

Responsibility SHALL persist across time as long as at least one of the following holds:

a) downstream impacts remain measurable,
b) the Subject continues to benefit from the originating action,
c) the Subject retains the capacity to mitigate, reverse, or limit further harm.

Termination, dissolution, or transformation of a Subject SHALL NOT invalidate historical attribution.

---

8. Cascading Impact Attribution

A Subject SHALL be considered causally responsible not only for direct first-order impacts, but also for downstream impacts when all of the following conditions are satisfied:

a) the downstream impact is causally linked through a traceable chain of state transitions measured under DKP-1-IMPACT-001,
b) the impact occurs within a declared or logically inferred impact horizon Δt,
c) the impact exceeds or materially contributes to at least one axiom-defined reference bound B_i.

Lack of foresight, predictability, or statistical expectation SHALL NOT negate responsibility.

---

9. Nonlinear Cascade Events

A **Nonlinear Cascade Event** is a state transition in which a small or localized initial impact produces a disproportionately large system-level effect through known physical, ecological, social, or informational feedback mechanisms.

Where such an event is detected:

- the originating Subject SHALL be fully causally linked to the cascade origin,
- responsibility MAY be distributed if multiple initiating actions are detected,
- rarity, novelty, or statistical improbability SHALL NOT constitute exemption.

---

10. Second- and Higher-Order Effects

Second-order effects arise from immediate reactions to an action.
Third-order effects arise from adaptive responses to second-order effects.

Such effects SHALL be attributed to the originating Subject when:

a) the effects are physically or informationally measurable, and
b) attribution does not require speculative modeling of intent or belief.

Responsibility decays only when causal linkage falls below Physical Truth Layer confidence thresholds.

---

11. Cultural and Cognitive Harm

Cultural and cognitive harm constitutes valid systemic impact when measurable indicators demonstrate:

a) persistent degradation of shared symbolic systems, language coherence, or knowledge transmission, or
b) sustained increases in population-level cognitive distortion, disinformation persistence, or loss of epistemic capacity.

Such harm SHALL be treated as a systemic externality even in the absence of immediate physical damage.

Attribution SHALL be proportional to:

- reach,
- persistence,
- amplification potential of the contributing action.

---

12. Non-Exemption Clause

No Subject SHALL be exempt from attribution based on:

- status,
- authority,
- jurisdiction,
- ideology,
- cultural or moral justification,
- delegation to automation,
- temporal delay between action and effect.

Responsibility follows causality, not hierarchy.

---

13. Cross-Layer Isolation

This protocol SHALL NOT:

- measure impact magnitude,
- evaluate justice or proportionality,
- assign sanctions or compensation,
- override or reinterpret outputs of DKP-1-IMPACT-001.

Violation constitutes a critical architectural breach.

---

14. Protocol Finality

Once finalized, this protocol is immutable.

Any modification requires:

- a new protocol identifier,

- explicit declaration of incompatibility,
- full-system simulation under DKP-8-SIMULATION.

Protocol Hash (SHA-256): **[to be inserted at freeze]**

END OF PROTOCOL

DKP-1-IMPACT-001

Impact Measurement Protocol

Version 1.0

---

1. Purpose

The Impact Measurement Protocol defines how changes in the **Physical State Vector S(t)** are transformed into **time-indexed, bounded, and auditable impact metrics**.

This protocol performs **measurement only**.
It does **not** interpret value, intent, utility, justice, responsibility, or policy.

---

2. System Position and Anchoring

This protocol operates:

- above DKP-0-ORACLE-001 (Physical Truth Layer),
- below DKP-1-IDENTITY-001 (Identity & Subject Protocol),
- below DKP-1-JUSTICE-001 (Justice Function Protocol),
- below all governance, economic, and enforcement protocols.

All inputs to this protocol MUST originate exclusively from **Physical Truth Layer outputs**.

All reference bounds $\mathbf{B_i}$ MUST be explicitly imported from:

- DKP-1-AXIOMS-001, or
- normatively defined Physical Truth Layer indices
  (e.g., biosphere survival thresholds anchored in Genesis Block constants).

This protocol is bound to **Genesis Block #0 (2025-12-10)**.

---

3. Scope

This protocol governs:

- measurement of state change between two physical states,
- time-indexed impact evaluation over an externally supplied horizon Δt,
- detection of boundary approach and boundary crossing,
- classification of reversibility and externality,
- production of structured, channel-separated impact outputs.

This protocol explicitly excludes:

- optimization, scoring, or weighting,
- aggregation across channels,
- decision-making or enforcement,
- attribution of responsibility,
- compensation logic,
- any form of utility or justice calculation.

---

4. Core Definitions

Physical State Vector S(t)

An immutable, time-indexed vector of measured physical variables produced by DKP-0-ORACLE-001.

Baseline State $S(t_0)$

The reference physical state prior to an evaluated change.

Observed State $S(t_1)$

The measured physical state after the evaluated change.

Impact Horizon Δt

A time interval supplied as an external parameter defining the evaluation window.

Impact Channel

A logically independent dimension of physical or informational impact.

Normatively declared impact channels include, but are not limited to:

- Biosphere Integrity
- Atmospheric Composition
- Human Health Proxies
- Resource Depletion
- Energy Balance
- Cognitive Integrity Proxies

- Cultural Continuity Indicators

Impact Vector $I_i(t_0 \rightarrow t_1, \Delta t)$

A channel-specific, bounded impact metric defined as normalized physical change.

Reference Bounds B_i

Invariant physical limits imported from DKP-1-AXIOMS-001 or Physical Truth Layer indices.

Reversibility Flag R_i

A boolean indicator of physical or informational irreversibility.

Externality Flag X_i

A boolean indicator of boundary-crossing impact.

Uncertainty Envelope U_i

A bounded confidence interval propagated from Physical Truth Layer uncertainty.

---

5. Measurement Principle

Impact is defined strictly as the **difference between two physical states**:

$S(t_0) \rightarrow S(t_1)$ over **Δt**

For each impact channel *i*, let $S_i(t)$ denote the projection of $S(t)$ onto channel *i*.

The protocol computes:

$$I_i = (S_i(t_1) - S_i(t_0)) / B_i$$

The resulting value is:

- unaggregated,
- dimensionless,
- auditable.

If $|I_i| \geq 1$, a boundary crossing SHALL be flagged.

No aggregation across channels is permitted.

---

6. Reference Bounds and Boundary Detection

Each impact channel SHALL declare its applicable reference bounds B_i.

Bounds MUST be:

- physically or informationally defined,
- immutable within this protocol,
- traceable to DKP-1-AXIOMS-001 or Physical Truth Layer indices.

The protocol SHALL detect:

- boundary approach,
- boundary crossing.

Bounds SHALL NOT be modified, normalized, or reinterpreted.

---

7. Reversibility Classification

For each impact channel, the protocol SHALL evaluate reversibility using formal criteria.

Criteria MUST be:

- explicit,
- physically or informationally grounded,
- binary in output.

Illustrative criteria MAY include:

- entropy increase beyond reversible regimes,
- irrecoverable loss of biospheric structures,
- irreversible phase transitions,
- permanent loss of cognitive or cultural capacity
  as verified via Physical Truth Layer data.

Subjective or intent-based assessments are forbidden.

---

8. Externality Detection

The protocol SHALL distinguish between **internal** and **external** impact.

System boundary SHALL default to **planetary scale** unless explicitly narrowed by higher-layer protocols.

Any detected boundary crossing SHALL set $\mathbf{X_i}$ **= True**.

Absence of an explicit boundary definition SHALL be treated as **full externality exposure**.

---

9. Uncertainty Propagation

Measurement uncertainty from Physical Truth Layer inputs SHALL be propagated into each impact channel.

Propagation SHALL be deterministic.

Illustrative methods MAY include:

- Bayesian ensembles,
- posterior confidence bands (e.g., ±3σ).

Uncertainty SHALL NOT be used to suppress, downgrade, or invalidate detected impact.

---

10. Outputs

For each impact channel *i*, the protocol outputs:

- $\mathbf{I_i}$ — impact vector,
- $\mathbf{B_i}$ — reference bound,
- $\mathbf{R_i}$ — reversibility flag,
- $\mathbf{X_i}$ — externality flag,
- $\mathbf{U_i}$ — uncertainty envelope.

No aggregated impact score SHALL be produced.

---

11. Cross-Layer Isolation Invariant

No higher-layer protocol may:

- alter reference bounds,
- suppress impact channels,
- override reversibility or externality flags,
- inject valuation, weighting, responsibility, or optimization logic.

Violation constitutes a **critical architectural breach**.

---

12. Protocol Finality

Once finalized, this protocol is immutable.

Any modification requires:

- a new protocol identifier,
- explicit declaration of incompatibility,
- full-system revalidation under DKP-8-SIMULATION.

Protocol Hash (SHA-256): **[to be inserted at freeze]**

---

13. Illustrative Example (Non-Normative)

Input

- Channel: Atmospheric Composition
- $S(t_0)$: CO_2 = 426.91 ppm
- $S(t_1)$: CO_2 = 427.00 ppm
- Δt: 1 hour
- B_i: 450 ppm

Output

- $I_i \approx 0.004$
- R_i = False
- X_i = False
- U_i = ±0.01 ppm

This example is illustrative only and not normative.

END OF PROTOCOL

DKP-1-JUSTICE-001

Justice Function Protocol (δίκη)

Version 1.0

---

1. Purpose

The Justice Function Protocol defines how measured impact and attributed responsibility are transformed into deterministic justice outcomes within the Dikenocracy system.

Justice is defined here as a function, not an institution, authority, ideology, or moral judgment.

This protocol computes consequences, not punishment.
It produces binding justice outputs, not discretionary decisions.

---

2. System Position

This protocol operates:

- **above DKP-1-IMPACT-001 (Impact Measurement Protocol),**
- **above DKP-1-IDENTITY-001 (Identity & Subject Protocol),**

- **below all economic, governance, security, and enforcement protocols.**

This protocol SHALL NOT access raw Physical Truth Layer data directly.

All inputs MUST be imported exclusively from:

- **DKP-1-IMPACT-001 outputs, and**
- **DKP-1-IDENTITY-001 attribution bindings.**

---

3. Core Inputs

For each evaluated action instance A, the protocol receives:

3.1 Impact Set

A channel-separated, unaggregated set of impact outputs produced by DKP-1-IMPACT-001:

- **I_i — impact magnitude per channel,**
- **B_i — reference bounds,**
- **R_i — reversibility flags,**
- **X_i — externality flags,**
- **U_i — uncertainty envelopes.**

3.2 Responsibility Binding

From DKP-1-IDENTITY-001:

- **identified Subject(s),**
- **responsibility weights per Subject,**
- **temporal persistence indicators,**
- **cascading and higher-order attribution flags.**

3.3 Normative Constraints

From DKP-1-AXIOMS-001:

- **priority ordering of protected domains,**
- **absolute prohibitions,**
- **minimum survival and stability thresholds,**
- **non-negotiable axiom-defined bounds.**

---

4. Justice Definition

Justice (δίκη) is defined as a deterministic mapping:

δίκη : (Impact, Responsibility, Axioms) → Consequence Vector C

The output vector C SHALL contain no:

- **moral language,**
- **intent interpretation,**

- **discretionary adjustment,**
- **subjective weighting.**

Justice outcomes are computed, not interpreted.

---

5. Justice Evaluation Domains

Justice SHALL be evaluated independently across the following domains:

1. **Restitution Domain**
2. **Restriction Domain**
3. **Isolation Domain**
4. **Exclusion Domain**

No domain SHALL be skipped if its triggering conditions are met.

---

6. Restitution Domain

Restitution applies when:

- **impact is reversible (R_i = True), and**
- **mitigation or repair is physically possible.**

The protocol SHALL compute:

- **required mitigation scope,**

- **proportional restitution obligations per Subject,**
- **time constraints for restitution completion.**

Restitution SHALL NOT exceed the measurable impact.

---

7. Restriction Domain

Restriction applies when:

- **impact exceeds axiom-defined safe margins, or**
- **repeated harmful behavior is detected, or**
- **mitigation capacity is insufficient.**

Restrictions MAY include:

- **limitation of action scope,**
- **throttling of resource access,**
- **enforced participation constraints.**

Restrictions MUST be:

- **proportional,**
- **reversible where physically possible,**
- **continuously re-evaluated.**

Restrictions SHALL NOT be used as punitive measures and SHALL exist solely to prevent further harm.

---

8. Isolation Domain

Isolation applies when:

- **impact is irreversible (R_i = False), or**
- **externality exposure is critical (X_i = True), or**
- **Subject behavior presents systemic risk.**

Isolation SHALL be:

- **functional, not punitive,**
- **targeted strictly at harm prevention,**
- **minimal in scope.**

Physical isolation SHALL be treated as a last-resort measure.

Isolation SHALL prioritize functional separation over physical confinement whenever technically feasible.

---

9. Exclusion Domain

Exclusion applies when:

- **a Subject persistently violates non-negotiable axioms, or**
- **mitigation and isolation fail to contain harm, or**
- **the Subject refuses or is incapable of compliance.**

Exclusion SHALL result in:

- **removal from system participation,**
- **loss of system-provided privileges,**
- **persistence of historical attribution.**

Exclusion SHALL NOT entail physical harm, lethal deprivation, or conditions leading to loss of life.

All exclusion outcomes MUST remain consistent with Axiom A1 (Preservation of Life) as defined in DKP-1-AXIOMS-001.

Exclusion terminates system participation and access to system-provided privileges only. It SHALL NOT authorize annihilation, abandonment, or indirect lethal exposure.

Exclusion is not annihilation and does not imply moral condemnation.

---

10. Proportionality and Distribution

Where multiple Subjects are responsible:

- **consequences SHALL be distributed proportionally to responsibility weights,**
- **no Subject SHALL absorb consequences exceeding its attributable contribution.**

Collective responsibility SHALL NOT nullify individual accountability.

---

11. Temporal Re-evaluation

Justice outputs SHALL be re-evaluated when:

- **impact metrics change,**
- **mitigation occurs,**
- **new data reduces uncertainty,**
- **system boundary conditions shift.**

Justice is adaptive but not discretionary.

Re-evaluation frequency SHALL be bounded by
Physical Truth Layer temporal guarantees.

Justice outputs MAY NOT be re-evaluated more frequently than the minimum
TTL (Time-To-Live) of the underlying Physical Truth Layer data
that produced the original impact measurements.

Any attempt to trigger re-evaluation using incomplete, stale,
or selectively withheld data SHALL be treated as continued exposure
to prior justice outcomes.

Adaptive justice SHALL NOT permit oscillatory relief,
temporary concealment, or strategic delay of mitigation.

---

12. No-Exemption Invariant

No Subject SHALL be exempt from justice outcomes based on:

- **status,**
- **authority,**
- **jurisdiction,**

- **ideology,**
- **cultural justification.**

Justice follows causality, not hierarchy.

---

13. Cross-Layer Isolation

This protocol SHALL NOT:

- **reinterpret impact metrics,**
- **alter identity attribution,**
- **override axiom-defined bounds,**
- **inject policy, governance, or moral reasoning.**

Violation constitutes a critical architectural breach.

---

14. Transparency and Auditability

All justice computations MUST be:

- **deterministic,**
- **reproducible,**
- **fully auditable,**
- **traceable to protocol inputs.**

Opaque, discretionary, or non-reproducible justice mechanisms are forbidden.

---

15. Protocol Finality

Once finalized, this protocol is immutable.

Any modification requires:

- **a new protocol identifier,**
- **explicit incompatibility declaration,**
- **full-system simulation under DKP-8-SIMULATION.**

Protocol Hash (SHA-256): [to be inserted at freeze]

END OF PROTOCOL

DKP-2-ASSETS-001

Property & Assets Protocol

Version 1.0

---

1. Purpose

The Property & Assets Protocol defines how assets, resources, and property rights are established, maintained, constrained, revoked, and reallocated within the Dikenocracy system.

Property is not treated as an absolute or intrinsic right.
It is defined as a **conditional, revocable allocation of control**, justified exclusively by measurable contribution and bounded by justice and physical reality.

This protocol ensures that:

- ownership reflects net justice contribution,
- accumulation cannot externalize harm,
- assets cannot be used to bypass axiomatic limits,
- property remains subordinate to impact, causality, and truth.

---

2. System Position

This protocol operates:

- strictly downstream of DKP-0-ORACLE-001 (Physical Truth Layer),
- above all L1 protocols (AXIOMS, IMPACT, IDENTITY, JUSTICE),
- alongside DKP-2-FINANCE-001,
- below social, labor, security, crisis, and infrastructure protocols (L3–L5).

All asset-related decisions are invalid in the presence of a Physical Truth Layer systemic halt or unresolved divergence.

---

3. Core Definitions

3.1 Asset

An **Asset** is any physical, informational, or infrastructural entity that:

- can be controlled, excluded, or transferred,

- produces measurable impact across one or more impact channels,
- enables production, accumulation, or systemic influence.

Assets include, but are not limited to:

- land and natural resources,
- infrastructure and machinery,
- informational and intellectual systems,
- productive capital and financial instruments,
- algorithmic, digital, or networked systems.

3.2 Property Right

A **Property Right** is a system-granted, conditional permission to control, use, or derive benefit from an Asset.

Property Rights are:

- non-absolute,
- non-permanent,
- continuously impact-contingent,
- subordinate to justice outcomes and axiomatic constraints.

---

4. Ownership Granting Conditions

A Property Right MAY be granted only if all of the following hold:

a) the Subject demonstrates non-negative net justice contribution,
b) projected asset use remains within impact bounds,

c) axiomatic priorities are not violated,
d) the Subject retains capacity for harm mitigation and restitution.

Ownership SHALL NOT be granted solely on the basis of:

- prior possession,
- inheritance without obligation transfer,
- contractual abstraction detached from measurable impact.

---

5. Conditionality and Persistence

Property Rights persist only while:

- justice contribution remains non-negative,
- asset use complies with impact constraints,
- restitution obligations are satisfied.

Failure of any condition SHALL trigger automatic degradation,
restriction, or suspension of the Property Right.

No Property Right is permanent.

---

6. Asset Use Constraints

Assets MUST NOT be used to:

- amplify irreversible harm,
- externalize damage beyond system boundaries,
- bypass justice or identity attribution,
- violate axiomatic priorities.

Asset use that increases systemic risk or irreversible damage
constitutes grounds for restriction or revocation.

---

7. Accumulation and Concentration Limits

Asset accumulation is subject to **impact-based concentration constraints**.

Where accumulation:

- increases systemic fragility,
- enables coercive dominance,
- amplifies irreversible or cascading harm,

the protocol SHALL trigger:

- graduated restrictions,
- enforced divestment,
- partial or full reallocation.

Concentration thresholds are derived from impact metrics,
not nominal valuation or market price.

---

8. Revocation and Reallocation

8.1 Revocation Triggers

Property Rights SHALL be revoked when:

- justice outcomes mandate Restriction, Isolation, or Exclusion,
- asset use causes irreversible or systemic harm,
- restitution obligations cannot be fulfilled.

Revocation is a **functional correction**, not punishment.

8.2 Reallocation Mechanisms

Revoked assets MAY be:

- placed under public stewardship,
- reassigned to alternative Subjects,
- transferred to reserve or mitigation pools.

Reallocation SHALL prioritize:

- harm mitigation,
- continuity of essential services,
- protection of axiomatic priorities.

Reallocation Transparency Constraint

All asset reallocation processes SHALL be:

- publicly observable,
- fully auditable,
- traceable to justice outcomes and impact constraints,
- executed via deterministic, rule-based procedures.

No discretionary authority, closed committee, or opaque administrative body MAY control or override asset reallocation.

Public stewardship denotes **algorithmic custodianship under open rules**, not bureaucratic management.

---

9. Natural and Critical Assets

Certain assets are designated as **Non-Privatizable** or **Conditionally Privatizable**, including:

- biosphere-critical systems,
- water, air, and ecological infrastructure,
- essential cognitive and informational commons.

Such assets MAY only be held under strict stewardship conditions and SHALL always remain revocable.

---

10. Transfer and Inheritance

Any transfer of property rights, including inheritance, requires:

- explicit transfer of justice obligations,
- acceptance of ongoing responsibility,
- compliance with current impact constraints.

Inheritance SHALL NOT erase historical attribution or exempt the recipient from justice outcomes.

---

11. Justice-Driven Asset Access Constraint

If a Subject is placed under Restriction, Isolation, or Exclusion per DKP-1-JUSTICE-001:

- control over non-essential assets SHALL be restricted or suspended,
- asset-derived benefits MAY be limited,

- access necessary for preservation of life SHALL be maintained in accordance with Axiom A1.

This protocol SHALL NOT override justice outcomes.

---

12. Transparency and Identity Binding

All asset ownership and control structures MUST be:

- registered,
- publicly auditable,
- directly and unambiguously bindable to Subjects as defined in DKP-1-IDENTITY-001.

Hidden ownership, shell abstractions, offshore structures, or any form of control that prevents causal attribution of impact or responsibility are forbidden.

Identity Binding Requirement

Any ownership abstraction that obstructs causal attribution SHALL be treated as invalid within the system.

This requirement is a necessary condition for the operation of DKP-1-IDENTITY-001 and cannot be waived.

---

13. Cross-Layer Isolation

This protocol SHALL NOT:

- redefine justice logic,
- alter impact measurements,
- introduce policy discretion,

- create exemptions from axiomatic constraints.

Violation constitutes a critical architectural breach.

---

14. Protocol Finality

Once finalized, this protocol is immutable.

Any modification requires:

- a new protocol identifier,
- explicit declaration of incompatibility,
- full-system simulation under DKP-8-SIMULATION.

Protocol Hash (SHA-256): **[to be inserted at freeze]**

END OF PROTOCOL

DKP-2-FINANCE-001

Financial System Protocol

Version 1.0

---

1. Purpose

The Financial System Protocol defines how financial activity — including savings, lending, credit issuance, investment, capital allocation, and pricing of capital — operates within the Dikenocracy system.

The protocol embeds **δίκη (justice as a function)** directly into financial mechanics, ensuring that:

- cost of capital reflects measured impact and responsibility,
- externalities are internalized deterministically,
- financial incentives align with long-term physical and social stability.

This protocol governs **economic mechanics**, not policy discretion.

It does **not**:

- create or manage fiat monetary regimes,
- override justice outcomes,
- perform subjective valuation or preference aggregation,
- substitute for governance or social support layers.

---

2. System Position

This protocol operates:

- above all L1 protocols
  (DKP-1-AXIOMS-001, DKP-1-IMPACT-001, DKP-1-IDENTITY-001, DKP-1-JUSTICE-001),
- below social, infrastructural, and intersystem protocols (L5–L6),
- alongside security and fail-safe mechanisms (L3–L4).

All financial computations MUST be traceable to:

- measured impact outputs (DKP-1-IMPACT-001),
- responsibility bindings (DKP-1-IDENTITY-001),

- justice outcomes (DKP-1-JUSTICE-001),
- axiomatic constraints (DKP-1-AXIOMS-001).

---

3. Core Economic Units

3.1 Capital Units (CU)

Capital Units (CU) are unitless, fungible representations of deployable economic capacity within the system.

CU represent **productive capability net of justice-weighted externalities**, not nominal wealth.

All CU flows are recorded on a deterministic, auditable ledger.

3.2 Justice-Weighted Cost of Capital (JWCoC)

The cost of capital is determined as a deterministic function of:

- historical justice outcomes associated with a Subject,
- projected impact risks across relevant channels,
- axiomatic reference bounds and safety margins.

Positive justice contribution reduces cost of capital.
Negative or risky impact exposure increases cost of capital.

There is no discretionary pricing of risk.

---

4. Time, Risk, and Capital Pricing

4.1 Justice-Anchored Interest

Interest rates are computed as a function of:

- justice burden carried by the borrower,
- impact volatility and externality exposure,
- reversibility and mitigation capacity.

Interest is **not compensation for impatience**,
but a pricing of **measured risk and justice imbalance**.

4.2 Time Value of Capital (Strict Constraint)

The system explicitly **rejects subjective time preference**.

Explicit Time Preference Prohibition

Subjective time preference, impatience discounting, or utility-based
devaluation of future outcomes SHALL NOT be used in any financial computation
within this protocol.

Temporal discounting is permitted **exclusively** as a consequence of
measurable changes in projected impact channels over time,
as defined by DKP-1-IMPACT-001.

For avoidance of doubt, the absence of subjective discounting does not imply zero time sensitivity.

Time remains a structurally relevant dimension through impact evolution, risk accumulation, reversibility decay, and exposure duration, all of which are evaluated via physically measurable impact channels rather than subjective preference functions.

This constraint is mandatory and reflects **Axiom A2**
(Intergenerational Responsibility) as defined in DKP-1-AXIOMS-001.

---

5. Credit and Lending

5.1 Credit Issuance

Credit MAY be issued only if:

a) projected justice-weighted productive output is sufficient for repayment,
b) expected impact does not violate axiomatic bounds,
c) aggregate exposure remains within systemic safety margins.

Credit is a **temporary imbalance**, not a right.

5.2 Credit Limits

Credit limits are dynamically computed based on:

- justice history of the Subject,
- projected impact correlation,
- systemic stress indicators.

No Subject may increase leverage if doing so raises the probability of axiom-bound violation.

---

6. Savings and Reserves

6.1 Savings

Savings are CU held in reserve and may generate returns derived from:

- duration of deployment,
- justice-weighted performance of deployed capital,
- measured systemic risk.

Savings returns are deterministic and fully auditable.

6.2 Systemic Reserve Pools (SRP)

Systemic Reserve Pools exist to:

- absorb defaults,
- fund restitution obligations,
- prevent cascading systemic failure.

Reserve sizing is impact-based, not percentage-based.

---

7. Investment and Capital Allocation

Capital allocation decisions SHALL be driven by:

- expected net justice output,
- impact risk envelopes,
- alignment with axiomatic priorities.

Speculative or purely price-driven allocation is forbidden.

---

8. Default and Financial Restitution

8.1 Default Conditions

A default occurs when:

- repayment cannot be achieved within a justice-defined horizon, and
- continued exposure threatens axiomatic bounds.

Defaults trigger **justice-defined outcomes**, not punishment.

8.2 Restitution Handling

Restitution MAY include:

- reserve deployment,
- obligation restructuring,
- proportional loss allocation.

Restitution is bounded by measurable damage and justice outcomes.

---

9. Leverage and Systemic Risk

Leverage SHALL be constrained such that:

- amplification of negative impact remains below safety thresholds,
- correlated failures cannot cascade beyond reserve capacity.

Leverage limits are impact-based, not volatility-based.

---

10. Interoperability with External Financial Systems

When interfacing with external systems:

- all values MUST be translated into justice-weighted internal equivalents,
- external risk MUST be fully internalized before deployment.

No external financial structure may bypass justice constraints.

---

11. Justice-Driven Financial Access Constraint

11.1 Automatic Suspension under Exclusion

If a Subject is assigned to the **Exclusion Domain**
under DKP-1-JUSTICE-001, all financial access governed by this protocol
SHALL be automatically suspended.

This suspension is **causal**, not discretionary,
and requires no independent financial evaluation.

The Financial System Protocol SHALL NOT:

- override exclusion outcomes,
- re-enable access under alternative criteria,
- provide compensatory financial pathways.

Financial access MAY be restored **only** upon formal exit from
the Exclusion Domain as determined by DKP-1-JUSTICE-001.

---

12. Transparency and Auditability

All financial mechanisms MUST be:

- deterministic,
- reproducible,
- fully auditable,
- traceable to L1 protocol outputs.

Opaque, discretionary, or proprietary financial logic is forbidden.

---

13. Cross-Layer Isolation

This protocol SHALL NOT:

- reinterpret impact measurements,
- override identity attribution,
- override justice outcomes,

- inject policy, ideology, or moral judgment.

Violation constitutes a critical architectural breach.

---

14. Protocol Finality

Once finalized, this protocol is immutable.

Any modification requires:

- a new protocol identifier,
- explicit declaration of incompatibility,
- full-system simulation under DKP-8-SIMULATION.

Protocol Hash (SHA-256): **[to be inserted at freeze]**

END OF PROTOCOL

DKP-2-LABOR-001

Labor & Participation Protocol

Version 1.0

---

1. Purpose

The Labor & Participation Protocol defines how participation in productive, restorative, and socially stabilizing activity is organized within the Dikenocracy system.

Labor is not treated as coercion, obligation, or moral duty.
It is defined as a **measurable mechanism for restoring and maintaining justice balance**, enabling Subjects to:

- contribute to system stability,
- access non-essential resources,
- recover from negative justice states,
- participate without ideological, political, or cultural conformity.

This protocol ensures that **no Subject is forced into labor to preserve life**, while preserving accountability for measurable impact.

---

2. System Position

This protocol operates:

- strictly downstream of DKP-0-ORACLE-001 (Physical Truth Layer),
- above all L1 protocols (AXIOMS, IMPACT, IDENTITY, JUSTICE),
- alongside DKP-2-FINANCE-001 and DKP-2-ASSETS-001,
- below crisis, security, social, and education protocols (L3–L5).

All participation rules are invalid during a PTL systemic halt or unresolved divergence.

---

3. Core Definitions

3.1 Labor

Labor is any voluntary, sustained activity that:

- produces measurable impact under DKP-1-IMPACT-001,

- contributes to restoration, maintenance, or protection of physical, social, or informational stability,
- can be causally attributed to a Subject.

Labor includes, but is not limited to:

- physical and infrastructural work,
- cognitive and creative activity,
- caregiving and social support,
- maintenance of critical knowledge and skills,
- restorative or preventive actions.

3.2 Participation

Participation is the voluntary engagement of a Subject in recognized labor or restorative activity.

Participation is evaluated exclusively through **measured impact**. Intent, belief, ideology, or declared motivation are irrelevant.

3.3 Contribution Record

A **Contribution Record** is an immutable, time-indexed entry linking:

- a Subject,
- a participation activity,
- measured impact outputs,
- resulting justice adjustment.

---

4. Baseline Access Guarantee

4.1 Non-Conditional Survival Access

Every Subject SHALL retain access to minimum life-preserving resources,
independent of labor participation, in accordance with
Axiom A1 (Preservation of Life).

No Subject may be deprived of:

- basic nutrition,
- shelter from lethal exposure,
- emergency medical assistance.

Baseline survival access SHALL NOT be contingent on labor,
obedience, loyalty, or economic productivity.

4.2 Baseline Does Not Neutralize Responsibility

Baseline access preserves life only.
It does NOT neutralize negative justice balance
or eliminate responsibility for harm.

Restoration of full participation and access requires
measurable contribution or restitution.

---

5. Participation and Justice Recovery

5.1 Voluntary Restoration Pathways

Subjects in a negative justice state SHALL be offered
voluntary participation pathways enabling recovery
through contribution.

These pathways MUST be:

- transparent,
- non-punitive,
- non-humiliating,
- scaled to Subject capacity and context.

Participation opportunities SHALL be plural and diverse,
preventing exploitation, monoculture, or forced specialization.

5.2 Justice Recovery Through Labor

Justice recovery is computed as a deterministic function of:

- measured impact of participation,
- relevance to harmed impact channels,
- time horizon of contribution.

Symbolic, performative, or purely declarative activity
SHALL NOT be recognized as labor.

---

6. Prohibited Labor Conditions

Labor participation SHALL NOT:

- be compulsory for survival,
- be used as punishment,
- involve debt bondage or open-ended obligation,
- require ideological, cultural, or political alignment,
- be assigned based on status, origin, or identity.

Forced labor constitutes a critical violation
of axiomatic constraints.

---

7. Allocation of Participation Opportunities

Participation opportunities SHALL be allocated based on:

- system needs derived from impact deficits,
- Subject capacity and explicit consent,
- avoidance of concentration, exploitation, or dependency.

No centralized authority MAY monopolize assignment.

All allocation procedures MUST be transparent,
auditable, and rule-based.

---

8. Compensation and Recognition

8.1 Justice-Linked Compensation

Compensation for participation MAY include:

- Capital Units (CU),
- access to assets or services,
- relaxation of justice-derived restrictions,
- partial or full restoration of participation rights.

Compensation is proportional to **measured impact**,
not hours worked, status, or bargaining power.

8.2 Non-Market and Socially Stabilizing Contributions

Non-market contributions SHALL be recognized as valid labor
when they produce measurable stabilizing impact, including:

- caregiving for dependents or vulnerable persons,
- maintenance of social cohesion and continuity,
- preservation, transmission, and safeguarding of knowledge,
- prevention of systemic degradation not captured by markets.

Such contributions address **otherwise invisible externalities**
and are evaluated using appropriate physical or informational proxies
under DKP-1-IMPACT-001.

---

9. Refusal, Exit, and Crisis Modulation

9.1 Right to Refuse Participation

Outside formally declared crisis conditions,
no Subject SHALL be compelled to participate in labor.

Refusal of participation:

- does not constitute a violation,
- does not trigger punishment,
- does not affect baseline survival access.

9.2 Crisis Modulation of Participation

During a formally declared crisis under DKP-4-CRISIS-001,
where failure of participation would threaten
systemic survival or collapse, the right to refuse
participation MAY be temporarily constrained.

Such constraints MUST:

- be strictly time-limited,
- be proportionate to the declared threat,
- preserve Axiom A1 (Preservation of Life),
- prioritize **Axiom A2 (Systemic Sustainability)**.

Crisis modulation SHALL NOT create permanent obligations
or post-crisis penalties.

---

10. Participation Under Restriction or Isolation

Subjects under Restriction or Isolation
per DKP-1-JUSTICE-001:

- MAY participate in limited or supervised activities,
- MUST retain pathways for justice recovery,
- SHALL NOT be exploited or coerced.

Participation remains voluntary outside crisis conditions.

---

11. Transparency and Identity Binding

All participation and contribution records MUST be:

- directly bindable to identifiable Subjects
(DKP-1-IDENTITY-001),
- publicly auditable,
- traceable to measured impact outputs.

Proxy, fictitious, or obscured participation is forbidden.

---

12. Cross-Layer Isolation

This protocol SHALL NOT:

- redefine justice logic,
- override impact measurements,
- function as punishment or discipline,
- introduce ideological criteria.

Violation constitutes a critical architectural breach.

---

13. Protocol Finality

Once finalized, this protocol is immutable.

Any modification requires:

- a new protocol identifier,
- explicit incompatibility declaration,
- full-system simulation under DKP-8-SIMULATION.

Protocol Hash (SHA-256): **[to be inserted at freeze]**

END OF PROTOCOL

DKP-3-ANTITERROR-001

Anti-Terror & Asymmetric Harm Containment Protocol

Version: 0.2.0
Status: Architecture Lock (Reviewer-integrated)
Layer: L3 – Anti-Terror / Asymmetric Threat Containment

---

0. Preamble

DKP-3-ANTITERROR-001 defines the protocol by which Dikenocracy responds to **asymmetric, non-state, non-linear harm mechanisms** commonly labeled as “terrorism”.

Within DKP, terrorism is **not an ideology, belief system, identity, or affiliation**. It is a **functional pattern of harm** characterized by:

- deliberate targeting of life (A1),
- asymmetric delivery of violence,
- intent to induce systemic instability beyond the immediate physical damage.

This protocol is strictly defensive and containment-oriented.

---

1. Purpose

The purpose of this protocol is to define how DKP detects, contains, and neutralizes **ongoing asymmetric harm streams** that:

- target civilians or protected domains,
- bypass conventional Defense symmetry,
- seek amplification through fear, randomness, or cascade effects,
- are confirmed by Physical Truth Layer (PTL).

ANTITERROR is not punitive and does not replace Justice.

---

2. System Position

This protocol operates:

- strictly downstream of DKP-0-ORACLE-001 (PTL) and DKP-0-TIME-001,
- downstream of DKP-1-IMPACT-001, DKP-1-IDENTITY-001, DKP-1-JUSTICE-001,
- after DKP-3-INTERNAL-SEC-001,
- after and in coordination with DKP-3-DEFENSE-001,

- upstream of DKP-4-CRISIS-001.

Hard constraints:

- SHALL NOT infer ideology, intent, belief, or affiliation.
- SHALL NOT apply collective responsibility.
- SHALL NOT operate without PTL-confirmed harm.
- SHALL NOT substitute Justice or Defense protocols.

---

3. Core Definitions

3.1 Terror Event (DKP Definition)

A Terror Event is any **PTL-confirmed asymmetric harm stream** that:

- targets non-combatant subjects or protected civilian domains,
- produces high systemic destabilization relative to physical scale,
- employs non-linear delivery methods (randomized, concealed, decentralized).

Systemic destabilization is defined functionally and MUST be measurable via DKP-1-IMPACT-001, including but not limited to:

- sharp entropy spikes in social or informational nodes,
- abrupt population mobility vector changes (panic dispersion),
- PTL-confirmed overload of civilian response or emergency channels.

“Terror” is a property of the harm pattern, not of the actor.

3.2 Asymmetric Harm Stream

An Asymmetric Harm Stream is a sequence of harm events where:

- the attacker is not a symmetric system participant,
- the harm delivery does not require territorial control,
- the damage propagates through fear, uncertainty, or infrastructure cascades.

3.3 Protected Civilian Domain

Protected Civilian Domains include:

- civilian populations and public spaces,
- civilian transport systems,
- hospitals, schools, shelters,
- food, water, and energy distribution nodes serving civilians.

---

4. Anti-Terror Invariants (Hard)

4.1 PTL Supremacy

No anti-terror action may occur without PTL-confirmed evidence of an ongoing terror event or asymmetric harm stream.

4.2 Non-Ideological Constraint

ANTITERROR SHALL NOT:

- profile beliefs, religions, ethnicities, or political views,
- infer intent from speech or association,
- treat identity as a risk signal.

Only physical/system harm patterns qualify.

4.3 Containment-Only Rule

ANTITERROR actions aim solely to:

- stop ongoing harm,
- prevent immediate recurrence,
- protect civilian life.

They do not seek punishment, deterrence through fear, or symbolic retaliation.

4.4 Minimal Necessary Force

All actions MUST be:

- proportional to the measured harm,

- localized to the threat vector,
- reversible where possible,
- immediately terminable when PTL confirms harm cessation.

---

5. Anti-Terror State Model (DTI-Governed)

- **T0 – No Terror Activity**
  - No PTL-confirmed asymmetric harm streams.
- **T1 – Active Terror Event**
  - PTL confirms an ongoing asymmetric harm stream targeting civilians.
  - Immediate localized containment actions permitted.
- **T2 – Sustained Asymmetric Threat**
  - Multiple or continuous terror events confirmed.
  - Coordinated multi-domain containment permitted.
- **T3 – Mass Casualty / Systemic Terror**
  - PTL confirms threat exceeding Defense capacity or mass-casualty risk.
  - Mandatory escalation to DKP-4-CRISIS-001.

States require continuous PTL refresh to persist.

---

6. Allowed Anti-Terror Actions

Permitted actions include:

- physical interdiction of active attackers,
- isolation of attack vectors (transport, access routes),
- emergency evacuation and sheltering of civilians,
- rapid neutralization of active harm sources,
- temporary spatial lockdowns strictly limited to the threat zone,
- emergency medical response coordination,
- temporary technical isolation of local information propagation channels to limit nonlinear panic amplification (signal amplitude containment, not content control).

Notes:

- Actions are reactive and event-scoped.
- Information isolation is technical and time-limited, not ideological or content-based.
- No long-term occupation or control is permitted.

---

7. Prohibited Actions (Hard Bans)

ANTITERROR SHALL NOT:

- conduct ideological screening,
- implement mass surveillance,
- impose collective punishment,
- detain subjects without PTL-confirmed active harm,
- use terror designation to suppress dissent,
- apply retrospective justification.

No successful containment outcome may be used to justify violation of axioms or absence of PTL evidence at the moment an action was initiated.

---

8. Interaction with Defense, Justice, and Impact

- ANTITERROR is a specialization of Defense for asymmetric civilian-targeted harm.
- Defense provides infrastructure shielding; ANTITERROR provides rapid civilian protection.
- All harm stream data and containment logs SHALL be forwarded to DKP-1-IMPACT-001 for damage assessment and externality accounting.
- Justice consumes PTL evidence and logs post-factum.
- ANTITERROR actions terminate automatically when PTL confirms threat cessation.

---

9. Escalation Rules

ANTITERROR MUST escalate to DKP-4-CRISIS-001 when:

- civilian casualty risk exceeds acceptable thresholds,
- terror events propagate system-wide,
- asymmetric threat overwhelms containment capacity,
- PTL signals systemic destabilization.

If PTL confirms systematic use of civilian or transport infrastructure for asymmetric harm delivery, RED-based economic isolation mechanisms MAY be triggered via downstream protocols, rendering such logistics economically non-viable.

---

10. Audit and Transparency

All actions MUST be:

- logged with PTL anchoring,
- indexed by DTI-Day,
- reviewable post-event,
- subject to Justice review.

---

11. Cross-Layer Isolation

DKP-3-ANTITERROR-001 SHALL NOT:

- modify economic protocols,
- impose sanctions,
- regulate speech or ideology,
- override Defense or Justice decisions.

---

12. Finality Clause

Once frozen:

- changes require a new protocol identifier,
- mandatory simulation under DKP-8-SIMULATION-001,
- explicit incompatibility declaration.

Protocol Hash (SHA-256): [to be inserted at freeze]

END OF PROTOCOL

DKP-3-DEFENSE-001

Defense & System Protection Protocol

Version: 0.3.2
Status: Architecture Lock (Reviewer-Integrated, Clean Copy)
Layer: L3 – Defense / Harm Containment

---

0. Preamble

DKP-3-DEFENSE-001 defines the external defense envelope of Dikenocracy.

Within DKP, Defense is not a political instrument, not a military doctrine, not a punitive mechanism, and not a means of ideological or population control. Defense is a strictly functional subsystem whose sole purpose is to prevent, stop, or contain **ongoing or physically inevitable Physical Truth Layer (PTL)-confirmed harm** affecting protected domains.

Defense exists to preserve admissible physical and systemic states under DKP axioms, primarily Axiom A1 (Preservation of Life) and Axiom A1a (Risk Symmetry and Voluntary Lethal Risk). Defense does not pursue victory, deterrence, punishment, dominance, or territorial outcomes.

Participation in any defensive activity involving lethal or permanently disabling risk is **strictly voluntary** and governed by DKP-1-AXIOMS-001.

This protocol is fully compatible with:

- DKP-0-ORACLE-001 (Physical Truth Layer)
- DKP-0-TIME-001 (DTI)
- DKP-1-AXIOMS-001
- DKP-1-IDENTITY-001
- DKP-1-IMPACT-001
- DKP-1-JUSTICE-001
- DKP-3-INTERNAL-SEC-001

---

1. Purpose

The Defense & System Protection Protocol defines how the system responds to **external physical, technical, or infrastructure violence** when:

- harm is actively occurring, or
- a physically inevitable harm event is confirmed by PTL.

The objective of Defense is to **stop the harmful interaction** and restore admissible system operation with minimal irreversible damage. Defense is not a conflict-resolution mechanism and does not attempt to determine legitimacy, intent, or fault.

---

2. System Position

This protocol operates:

- strictly downstream of DKP-0-ORACLE-001 (PTL) and DKP-0-TIME-001,
- downstream of DKP-1-IDENTITY-001, DKP-1-IMPACT-001, and DKP-1-JUSTICE-001,
- **concurrently with DKP-3-INTERNAL-SEC-001, using priority synchronization**,
- in parallel with domain-specific security protocols where applicable,
- upstream of DKP-4-ERROR-001 and DKP-4-CRISIS-001.

Hard constraints:

- Defense SHALL NOT compute justice outcomes.
- Defense SHALL NOT assign guilt or interpret intent.
- Defense SHALL NOT impose punishment, sanctions, or political control.
- Defense SHALL NOT redefine Physical Truth or override axioms.

---

3. Core Definitions

3.1 Defensive Action

A Defensive Action is any physical or technical intervention whose sole function is to:

- stop,
- block,
- shield,
- isolate, or
- neutralize

an **ongoing or physically inevitable PTL-confirmed harm stream** within a protected domain.

3.2 External Harm Event

An External Harm Event is a situation in which:

- the source of harm lies outside the controlled execution boundary of DKP, and
- the interaction produces or will unavoidably produce measurable harm under DKP-1-IMPACT-001.

The term “external” is functional, not geopolitical.

3.3 Protected Domains

Protected Domains are the minimal set of targets for which Defense may be invoked:

- subject life and bodily integrity (A1 priority),
- critical DKP execution infrastructure (PTL, identity binding, audit, ledger integrity),
- critical biospheric nodes defined under Impact protocols,
- explicitly registered critical public infrastructure.

3.4 Verified Collective Security Risk

A Verified Collective Security Risk exists when PTL confirms that participation in a Defensive Action exposes a subject to a non-trivial probability of:

- bodily injury,
- permanent impairment, or
- death.

Risk verification is PTL-anchored and SHALL NOT depend on role labels, institutional affiliation, or declared status.

3.5 Voluntary Defense Participant

A Voluntary Defense Participant is a subject who:

- has given explicit and revocable consent to participate in a Verified Collective Security Risk,
- meets qualification and safety thresholds defined by subordinate protocols,
- is registered under DKP-1-IDENTITY-001 as a voluntary defense actor.

3.6 Vector of Physical Inevitability

A Vector of Physical Inevitability is a PTL-confirmed state in which current measured physical parameters (including trajectory, velocity, energy, or process initiation state) imply that, **absent intervention**, a Harm Event will occur with near-certainty within a finite time horizon.

Actions taken to interrupt or terminate a Vector of Physical Inevitability are classified as Defense actions, not preemptive actions.

---

4. Defense Invariants (Hard)

4.1 PTL Supremacy

No Defensive Action is permitted without PTL-confirmed evidence of an active or physically inevitable harm stream.

4.2 Non-Preemptive Constraint (Epistemic)

Defense SHALL NOT be initiated based on:

- forecasts or speculative predictions,
- intelligence assessments detached from PTL,
- political claims,
- statistical risk projections,
- narrative threat models.

Actions based on PTL-confirmed Vectors of Physical Inevitability do not constitute preemption.

4.3 Containment-Only Rule

Defense actions are limited to stopping the harmful interaction and restoring admissible operation.

Defense SHALL NOT pursue retaliation, deterrence, territorial gain, or dominance as objectives.

4.4 Minimal Necessary Action

Defensive Actions MUST be:

- minimal in scope,
- proportionate to measured harm,
- localized to the protected domain **and/or the physical harm source**,
- reversible where physically and logically possible.

4.5 No Justice Substitution

Defense does not replace Justice. It produces evidence, not verdicts.

4.6 Voluntary Participation Constraint

No Defensive Action involving Verified Collective Security Risk may be assigned, imposed, or expected of any subject without explicit consent.

Refusal to participate:

- SHALL NOT trigger sanctions,
- SHALL NOT reduce baseline civil rights,
- SHALL NOT constitute disloyalty, violation, or fault.

---

5. Defense State Model (DTI-Governed)

Defense operates as a finite-state system indexed by DKP time:

D0 – No Defense
No PTL-confirmed external harm or inevitability vector.

D1.5 – Alert (Imminent Harm)
PTL confirms perimeter violation, hostile system activation, or a Vector of Physical Inevitability. Passive and protective measures are permitted, including shielding, evacuation, redundancy activation, and readiness escalation. No lethal engagement is implied.

D1 – Active External Harm
PTL confirms an active harm stream. Localized defensive actions permitted.

D2 – Sustained Harm
PTL confirms repeated or continuous harm. Expanded containment permitted within hard constraints.

D3 – Existential Threat
PTL confirms harm exceeding axiomatic thresholds (A1/A2) or threat to systemic survival. Mandatory escalation to DKP-4-CRISIS-001.

Defense SHALL NOT remain in D1.5, D2, or D3 without continuously refreshed PTL confirmation.

---

6. Allowed Defensive Actions

Allowed actions are strictly those that physically stop or contain harm, including but not limited to:

- physical shielding or hardening of protected nodes,
- interception or disruption of harm-delivery vectors,
- disconnection of harm-delivery channels,
- isolation or quarantine of compromised segments,
- evacuation and safe routing of subjects,
- emergency redundancy activation for critical DKP infrastructure.

6.1 Neutralization Boundary Rule

Neutralization of a harm source is permitted **only** insofar as it is the minimal physical operation required to terminate an active or inevitable harm stream.

Neutralization MAY occur at the physical location of the harm source when there is no other physically feasible method to terminate the harm stream within the admissible time horizon.

Neutralization SHALL NOT:

- create a new independent harm objective,
- be framed, recorded, or executed as retaliation,
- include persistent presence, governance, or occupation.

Any action involving Verified Collective Security Risk MAY ONLY be executed by Voluntary Defense Participants.

---

7. Prohibited Actions (Hard Bans)

Defense SHALL NOT be used for:

- speculative or narrative-based preemptive strikes,
- collective responsibility or punishment,
- retaliation as an objective,
- territorial capture or permanent occupation,
- economic punishment or sanctions,
- forced political alignment or governance.

Any such use constitutes a protocol breach.

---

8. Interaction with Justice, Identity, and Risk Symmetry

Defense does not determine legitimacy or fault.

Defense produces PTL-anchored evidence usable by DKP-1-JUSTICE-001.

When PTL confirms an identifiable external harm source, Defense logs SHALL automatically generate a **Resource Recovery Claim** routed to DKP-1-JUSTICE-001 for adjudication of restitution and cost recovery. Defense itself SHALL NOT pursue compensation.

Participation or non-participation in Verified Collective Security Risk SHALL be forwarded to DKP-1-IDENTITY-001 and DKP-2-FINANCE-001 **solely for risk-symmetry accounting and compensation logic**, without moral, punitive, or reputational interpretation.

Defense automatically winds down when:

- PTL confirms the harm stream has ceased or been neutralized, and
- admissible system states are restored.

---

9. Escalation Rules

Defense MUST escalate to DKP-4-CRISIS-001 when PTL confirms:

- axiomatic boundary breach risk,
- insufficiency of defensive measures,
- systemic or cascading harm beyond containment capacity.

---

10. Audit, Transparency, and Evidence Commitments

Every Defensive Action MUST be:

- indexed by DTI,
- anchored to PTL evidence,
- logged in a tamper-evident manner.

Defense logs SHALL be publicly verifiable **post-factum** under transparency, delay, and redaction rules defined by higher-layer governance and audit protocols.

---

11. Cross-Layer Isolation

DKP-3-DEFENSE-001 SHALL NOT:

- alter economic rules,
- introduce sanctions,
- govern information flows,
- manage populations,
- override Impact or Justice computations.

Defense is containment, not governance.

---

12. Finality Clause

Once frozen:

- any modification requires a new protocol identifier,
- explicit incompatibility declaration,
- mandatory system simulation under DKP-8-SIMULATION-001,
- public disclosure under transparency rules.

Protocol Hash (SHA-256): [to be inserted at freeze]

END OF PROTOCOL

DKP-3-INTERNAL-SEC-001

Internal Security & System Integrity Protocol

Version: 1.0

---

1. Purpose

The Internal Security & System Integrity Protocol defines how the Dikenocracy system preserves its internal coherence, correctness, and causal integrity in the presence of errors, manipulation attempts, or hostile actions.

Internal Security within DKP is **not** defined as surveillance, prediction, profiling, or ideological control. It is defined strictly as a functional mechanism for:

- detecting integrity violations anchored in Physical Truth Layer (PTL) outputs,
- containing ongoing or imminent system damage,
- preventing further distortion of Impact, Identity, Justice, or Economic execution,
- escalating unresolved or systemic compromise to Fail-Safe protocols.

This protocol exists to protect **system truth, causal attribution, and execution correctness**, not to judge intent, belief, or loyalty.

---

2. System Position

This protocol operates:

- strictly downstream of DKP-0-ORACLE-001 (Physical Truth Layer),
- downstream of DKP-1-IDENTITY-001, DKP-1-IMPACT-001, DKP-1-JUSTICE-001,
- in coordination with DKP-2-FINANCE-001, DKP-2-ASSETS-001, DKP-2-LABOR-001,
- upstream of DKP-3-DEFENSE-001 and DKP-3-ANTITERROR-001,
- upstream of DKP-4-ERROR-001 and DKP-4-CRISIS-001.

This protocol SHALL NOT:

- redefine Physical Truth,
- reinterpret Impact measurements,
- compute Justice outcomes,
- revoke rights or privileges autonomously,
- introduce punishment logic,
- override axiomatic constraints.

All restrictive or corrective effects affecting Subjects SHALL occur exclusively via formal input triggers submitted to DKP-1-JUSTICE-001 or DKP-1-IDENTITY-001, never by direct execution at L3.

---

3. Core Definitions

3.1 Integrity Violation

An Integrity Violation is any detectable deviation between:

- PTL-confirmed physical state,
- protocol-governed system state,
- and executed system behavior,

where such deviation:

- distorts attribution, impact measurement, justice computation, or execution,
- enables unaccountable or non-auditable state transitions,
- or threatens axiomatic bounds.

Integrity Violations are functional conditions, not moral assessments.

3.2 Internal Threat (DKP-Specific)

An Internal Threat is any Subject, process, or subsystem that:

- attempts to falsify or suppress PTL inputs or outputs,
- attempts to spoof, fragment, or obscure Identity attribution,
- attempts to manipulate Impact measurement pipelines,
- attempts to bypass or override Justice outcomes,
- attempts to corrupt audit trails or execution logs,

and produces or imminently enables an Integrity Violation.

Intent, ideology, affiliation, or declared motivation SHALL NOT be considered.

3.3 Evidence

Evidence is defined exclusively as cryptographically verifiable commitments anchored to the Physical Truth Layer and ultimately to Genesis Block #0.

Admissible evidence includes:

- PTL-signed data hashes,
- cryptographic commitments recorded in immutable ledgers,
- execution traces whose hashes are anchored to PTL time indices.

Evidence MUST be:

- auditable and reproducible,
- temporally indexed using DTI-Day (DKP-0-TIME-001),
- immune to discretionary suppression by virtue of cryptographic anchoring,
- traceable to Genesis Block #0 and Proof-of-Synergy consensus rules.

---

4. Core Invariants

4.1 PTL Supremacy

No internal security action may redefine or override Physical Truth Layer outputs.
Security actions MAY only respond to PTL-confirmed states or PTL-confirmed divergence.

4.2 Non-Preemptive Constraint

No coercive or restrictive action MAY be initiated based on:

- prediction,
- inferred intent,
- ideological alignment,
- statistical profiling,
- speculative risk modeling.

Only PTL-evidenced, already occurring integrity violations or active attempts to write invalid or unauthorized state transitions qualify as valid triggers.

4.3 Minimal Necessary Action

All security actions MUST be:

- strictly proportional to the detected integrity loss,
- limited in scope and duration,
- sufficient only to stop ongoing or imminent damage.

Permanent or expansive actions require escalation to higher layers.

4.4 Auditability and Reversibility

All actions under this protocol MUST be:

- logged immutably,
- traceable to triggering evidence,
- reversible where physically and logically possible.

Irreversible actions require elevated authorization thresholds and justification.

---

5. Security State Model

The Internal Security layer operates as a finite-state system governed by Dikenocratic Time (DKP-0-TIME-001).

- **S0 – Normal Operation**
  No detected integrity anomalies.
- **S1 – Suspicion**
  Non-coercive evidence collection and heightened verification.
  Maximum duration: 7 DTI-Days.

- **S2 – Confirmed Integrity Violation**
  Targeted containment actions permitted.
  Maximum duration: 14 DTI-Days unless escalated.
- **S3 – Active Compromise**
  Partial system isolation or execution throttling permitted.
  Maximum duration: 3 DTI-Days.
- **S4 – Systemic Compromise**
  Mandatory escalation to DKP-4-CRISIS-001.

State transitions MUST be evidence-driven, auditable, and automatically reverted to S0 upon expiration of the maximum duration unless escalated.

---

6. Triggers (PTL-Anchored)

Integrity response MAY be triggered only by:

- Identity Integrity Trigger: PTL-confirmed mismatch in attribution or credential binding,
- Impact Integrity Trigger: PTL-confirmed manipulation or suppression of impact channels,
- Justice Execution Trigger: unauthorized alteration or bypass of justice outcomes,
- Audit Integrity Trigger: PTL-confirmed log tampering or execution opacity.

Any Physical Truth Layer divergence or oracle inconsistency SHALL be handled exclusively by DKP-0-ORACLE-001. Upon PTL halt or arbitration flag, all L3 execution MUST immediately suspend and defer to L0 resolution.

---

7. Allowed Actions by State

7.1 S1 – Suspicion

Permitted actions:

- evidence preservation,
- increased verification frequency,
- mandatory transaction multi-signature requirement for sensitive or high-impact operations,
- challenge-response procedures via Identity protocol.

No artificial throttling, economic slowdown, or discretionary limitation of baseline access is permitted at this stage.

7.2 S2 – Confirmed Integrity Violation

Permitted actions:

- scoped privilege revocation (Identity-bound),
- isolation of affected subsystems,
- temporary freeze of disputed transactions or assets,
- initiation of Justice-domain workflows.

7.3 S3 – Active Compromise

Permitted actions:

- partial execution halt of compromised modules,
- forced safe-mode execution,
- mandatory multi-party authorization for sensitive operations.

7.4 S4 – Systemic Compromise

Mandatory actions:

- escalation to DKP-4-CRISIS-001,
- request for PTL systemic halt where applicable,
- suspension of non-essential execution paths.

---

8. Prohibited Actions (Hard Bans)

This protocol SHALL NOT permit:

- mass surveillance without PTL trigger,
- collective punishment or guilt by association,
- permanent exclusion without Justice-domain outcome,
- secrecy of rules or hidden enforcement logic,
- security actions justified by ideology or narrative,
- concentration of Internal Security execution control.

No Subject, nor any Identity-linked group of Subjects, MAY control more than **4%** of nodes executing DKP-3-INTERNAL-SEC-001 logic, as defined by oracle and control concentration limits
in DKP-0-ORACLE-001.

Violation constitutes a critical architectural breach.

---

9. Due Process and Appeals

All restrictive actions MUST explicitly define:

- triggering PTL evidence,
- violated invariant or integrity rule,
- applied containment scope,
- reversal and appeal conditions under Justice protocol.

---

10. Cross-Layer Interfaces

This protocol interfaces with:

- Identity: attribution, revocation, revalidation,
- Impact: pipeline integrity verification,
- Justice: consequence computation and escalation,
- Finance & Assets: freeze / restore semantics,
- Infrastructure & Audit (L8): immutability and verification.

---

11. Protocol Self-Tests

The following invariants MUST always hold:

- No PTL evidence → no coercive action,
- Minimal sufficient containment,
- Complete audit trail,
- Preference for reversibility,
- No cross-layer authority overreach.

---

12. Versioning and Finality

This protocol is mutable until frozen.

Once finalized:

- any modification requires a new protocol identifier,
- explicit incompatibility declaration,
- full-system simulation under DKP-8-SIMULATION.

Protocol Hash (SHA-256): [to be inserted at freeze]

END OF PROTOCOL

DKP-3-POLICE-001

Public Order & Physical Enforcement Protocol

Version: 1.0
Status: Draft
Layer: L3 — Security / Enforcement

---

0. Preamble

DKP-3-POLICE-001 defines the strictly limited role, authority, and constraints of policing within Dikenocracy.

Policing is treated as a physical enforcement interface, not as a moral authority, investigative ideology, or discretionary power structure.

The sole function of police within DKP is to:

prevent immediate physical harm,

enforce PTL-verified prohibitions,

execute system decisions already determined by higher layers,

preserve public order without interpretation of intent, belief, or ideology.

Police do not define law, policy, justice, guilt, or truth.

---

1. Purpose

The purpose of DKP-3-POLICE-001 is to:

formalize policing as a bounded execution layer,

prevent discretionary or ideological policing,

eliminate predictive, pre-emptive, or belief-based enforcement,

ensure physical enforcement is always causally attributable,

protect Subjects from abuse of coercive power.

---

2. System Position

DKP-3-POLICE-001 operates:

downstream of DKP-0-ORACLE-001 (Physical Truth Layer),

downstream of DKP-1-AXIOMS-001,

downstream of DKP-1-IDENTITY-001,

downstream of DKP-1-IMPACT-001,

upstream of DKP-4-CRISIS-001 (only for escalation),

constrained by DKP-7-SCOPE-001.

Police actions SHALL NOT:

create new norms,

reinterpret axioms,

define guilt or liability,

operate outside PTL-confirmed conditions.

---

3. Definition of Police Authority

Police authority is defined as temporary, localized, and execution-only.

Police MAY:

physically intervene to stop ongoing or imminent PTL-verified harm,

enforce access restrictions already determined by system protocols,

detain Subjects only under conditions defined in this protocol,

secure physical scenes for PTL data capture.

Police SHALL NOT:

conduct ideological, moral, or preventive enforcement,

act on suspicion, profiling, or predictive scoring,

interpret intent, belief, loyalty, or motivation,

issue binding judgments.

---

4. Trigger Conditions for Police Action

Police action is permitted only when at least one of the following holds:

1. Active Physical Harm

Ongoing or imminent physical harm verified by PTL inputs.

2. System Execution Order

A valid enforcement order produced by L2 or L4 protocols.

3. Critical Infrastructure Protection

Immediate threat to PTL infrastructure, identity continuity, or essential biospheric systems.

Absence of PTL confirmation SHALL default to non-intervention.

---

5. Detention and Use of Force

5.1 Detention

Temporary detention is permitted only to:

stop active harm,

prevent immediate recurrence,

ensure identity attribution.

Detention SHALL:

be time-limited,

be logged immutably,

trigger automatic review by higher layers.

Preventive or indefinite detention is forbidden.

5.2 Use of Force

Use of force is permitted only when:

non-forceful alternatives are unavailable or ineffective,

force is proportional to the verified physical threat,

action minimizes irreversible harm (Axiom A4).

Lethal force is permitted only under Axiom A1 minimum-required conditions, as defined exclusively by DKP-4-CRISIS-001.

---

6. Accountability and Attribution

All police actions:

MUST be identity-attributed under DKP-1-IDENTITY-001,

MUST be PTL-logged,

MUST be auditable post-facto.

Police officers are not sovereign actors. Responsibility for any action is always traceable to:

the executing officer,

the issuing protocol or authority,

the originating Subject where applicable.

---

7. Prohibited Policing Functions

The following are explicitly forbidden:

predictive policing,

profiling based on ideology, religion, culture, or belief,

enforcement of morality or social norms,

surveillance not anchored in PTL necessity,

discretionary expansion of authority.

Violation constitutes a critical integrity breach.

---

8. Crisis Interaction

During a formally declared Crisis under DKP-4-CRISIS-001:

police authority MAY be temporarily extended,

such extension MUST be explicitly scoped,

no crisis action creates precedent.

All crisis policing actions remain constrained by DKP-7-SCOPE-001.

---

9. Transparency and Review

All policing statistics:

SHALL be publicly auditable in aggregated form,

SHALL preserve individual privacy,

SHALL support post-incident causal reconstruction.

No secret policing authority is permitted.

---

10. Scope Limitations

DKP-3-POLICE-001 SHALL NOT:

regulate belief, speech, or culture,

substitute judicial or justice protocols,

define long-term punishment or rehabilitation,

override exit rights or identity continuity.

---

11. Finality Clause

Once frozen:

any modification requires a new protocol identifier,

mandatory simulation under DKP-8-SIMULATION-001,

explicit compatibility declaration with DKP-1-AXIOMS-001 and DKP-7-SCOPE-001.

END OF PROTOCOL

DKP-4-CRISIS-001

Crisis & Fail-Safe Protocol

Version: 1.1
Status: Architecture Lock (Defense-Aligned Rewrite)
Layer: L4 – Crisis / Fail-Safe

---

0. Preamble

DKP-4-CRISIS-001 defines the system-wide fail-safe mode of Dikenocracy.

Crisis mode is invoked exclusively when normal protocol execution is insufficient to preserve axiomatic integrity, system survival, or admissible physical states, **as confirmed by Physical Truth Layer (PTL) evidence and downstream L3 escalation**.

This protocol governs exceptional conditions, not routine governance. It exists to prevent irreversible collapse, uncontrolled escalation, or loss of Physical Truth. Crisis handling in DKP is algorithmic, time-bounded, scope-limited, and authority-minimized.

Crisis mode does not create new powers. It temporarily constrains execution pathways to preserve survival and reversibility.

Crisis execution within DKP is non-normative by definition.

Any action, restriction, suspension, or authority exercised under this protocol SHALL NOT create precedent, custom, interpretation rule, or future authorization outside an explicitly declared Crisis Scope.

> Crisis actions SHALL NOT be interpreted post-factum as evidence of normal system capability, acceptable governance practice, or latent authority.
> Post-crisis normalization by interpretation is explicitly forbidden.

---

1. Purpose

The purpose of this protocol is to:

- preserve Axiom A1 (Preservation of Life) and Axiom A2 (Systemic Sustainability) under extreme conditions,
- prevent cascading failure across layers,
- enforce safe degradation rather than collapse,

- provide deterministic exit paths back to admissible operation, controlled upgrade, or system termination.

Crisis mode prioritizes survival, containment, and reversibility over optimization, efficiency, or growth.

All Crisis execution operates strictly within a Crisis Scope Envelope.

The Crisis Scope Envelope is a hard operational subset of DKP-7-SCOPE-001 and defines the maximal permissible actions, authorities, and interpretations allowed during Crisis execution.

The Crisis Scope Envelope SHALL NOT be expanded, inferred, or bypassed under any circumstances.

The Crisis Scope Envelope exists exclusively within S1 (Conditionally Applicable Domain) as defined in DKP-7-SCOPE-001.

Entry into Crisis Scope SHALL NOT elevate system applicability beyond S1 under any conditions.

---

2. System Position

This protocol operates:

- strictly downstream of DKP-0-ORACLE-001 (PTL) and DKP-0-TIME-001,
- downstream of all L1–L3 protocols,
- downstream of DKP-4-ERROR-001,
- **only upon escalation from DKP-3-DEFENSE-001 or equivalent L3 containment protocols**,
- upstream of DKP-4-UPGRADE-001 (when recovery is possible).

Hard constraints:

- DKP-4-CRISIS-001 SHALL NOT redefine axioms.
- DKP-4-CRISIS-001 SHALL NOT introduce new rights, obligations, or authorities.
- DKP-4-CRISIS-001 SHALL NOT operate without PTL anchoring.

Crisis execution is strictly bounded by DKP-7-SCOPE-001.

No Crisis logic, exception, or emergency interpretation may override, reinterpret, or extend system applicability beyond the limits defined in DKP-7-SCOPE-001.

Scope Constraint:
All actions executed under DKP-4-CRISIS-001 SHALL be strictly limited by the applicability boundaries defined in DKP-7-SCOPE-001.

No crisis condition, trigger, state, or action SHALL be extrapolated, generalized, or reused outside the explicitly declared Crisis Scope.

---

3. Crisis Definition

A Crisis is a PTL-confirmed system state in which **L3 containment and correction mechanisms are insufficient** to prevent imminent or ongoing violation of Axiom A1 or Axiom A2.

Crisis conditions include:

- sustained D3 (Existential Threat) states in DKP-3-DEFENSE-001 or equivalent,
- cascading errors exceeding local and regional correction capacity,
- loss, divergence, or instability of PTL integrity,
- multi-domain failures threatening life or system survival,
- undefined or non-deterministic execution states outside protocol specification.

Crisis is a system condition, not a political declaration, emergency order, or discretionary judgment.

---

4. Crisis Triggers (PTL-Anchored)

Crisis mode SHALL be entered when one or more of the following conditions are PTL-confirmed:

- sustained D3 state escalation from DKP-3-DEFENSE-001,
- sustained T3 state escalation from domain-specific Anti-Terror protocols,
- cascading systemic failure escalated from DKP-4-ERROR-001,
- verified loss or divergence of PTL outputs beyond correction tolerance,
- simultaneous multi-domain harm exceeding axiomatic survival margins.

Crisis SHALL NOT be initiated by forecast, policy decision, political authority, or human discretion.

---

5. Crisis State Model (DTI-Governed)

Crisis operates as a finite-state system indexed by DKP time:

C0 – Normal Operation
No crisis conditions present.

C1 – Emergency Containment
Immediate life-preserving actions activated.
Strict prioritization of survival-critical resources.

C2 – System Degradation Mode
Non-essential functions suspended.
Core execution isolated to preserve determinism and truth continuity.

C3 – Fail-Safe Isolation
Maximum containment enforced.
External interfaces minimized.
Cross-domain propagation halted.

C4 – Terminal Resolution
Controlled shutdown, irreversible isolation, or system partition executed to preserve Physical Truth and prevent uncontrolled collapse.

State persistence in C1–C4 requires continuous PTL confirmation and periodic revalidation.

---

6. Crisis Actions (Allowed)

During Crisis mode, the system MAY:

- suspend non-essential economic, informational, and optimization functions,
- enforce strict resource rationing **solely to preserve life and core execution**,
- isolate or quarantine failing subsystems, regions, or interfaces,
- activate autonomous infrastructure, energy, and sustainment reserves,
- freeze non-critical state transitions,
- prioritize PTL, audit, and identity continuity,
- activate Crisis Mercy Mode for non-anthropogenic events (e.g., solar storms, geological phenomena), allowing limited extension of oracle data TTLs to prevent false system halts while preserving life-support continuity.

All Crisis actions MUST be:

- proportional to verified threat,

- strictly time-limited,
- fully auditable,
- reversible where physically and logically possible.

Non-Precedent Rule:

Any action executed under Crisis mode SHALL NOT create normative precedent.

Such actions SHALL NOT be cited, reused, generalized, or referenced as justification for:

- non-crisis operation,
- protocol interpretation,
- governance logic,
- system upgrades.

Authority minimization during Crisis is a structural invariant, not a parameterized control function.

No numerical values, thresholds, coefficients, timers, decay curves, or quantitative authority limits MAY be defined in this protocol.

All numerical parameters governing Crisis authority duration, decay behavior, revalidation cadence, or exit sensitivity SHALL be defined, tested, and validated exclusively under DKP-8-SIMULATION-001.

---

7. Crisis Prohibitions (Hard Bans)

Even during Crisis, the system SHALL NOT:

- suspend Physical Truth Layer logging,
- grant discretionary authority to individuals or groups,
- override Justice axioms or identity attribution,
- conceal actions or decisions from audit,
- use Crisis as justification for permanent control or emergency governance,
- apply utilitarian valuation of human life.

Resource allocation algorithms SHALL NOT prioritize Subjects based on social status, historical impact, or perceived utility.

Allocation MUST be either:

- egalitarian (baseline survival minimum), or
- strictly determined by physical proximity and feasibility of survival resources.

Axiom A1 Interpretation Constraint

Interpretation of “minimum required conditions” under Axiom A1 SHALL NOT be inferred, extended, or operationalized by Crisis execution logic or by any operational, economic, or enforcement mechanism.

Such interpretation is permitted **only** within the Crisis Scope explicitly defined in DKP-7-SCOPE-001.

---

8. Governance During Crisis

Crisis governance is algorithmic only.

No emergency human authority is created.

All Crisis actions derive from pre-defined protocol logic.

Any human intervention SHALL be logged and treated as an external perturbation subject to post-crisis audit.

---

9. Exit Conditions

Crisis mode MUST terminate automatically when PTL confirms that:

- admissible physical and system states are restored,
- cascading failures are resolved or contained below crisis thresholds,
- Defense and Anti-Terror states return below existential levels,
- DKP-4-ERROR-001 confirms correction completeness.

Exit pathways include:

- **Sequential Recovery (Soft Reset):** controlled reactivation in strict order L0 → L1 → L2, where financial execution SHALL NOT resume until Justice confirms closure of crisis-originated claims,
- transition to DKP-4-UPGRADE-001,
- controlled system partition or termination.

Crisis state persistence beyond validated PTL windows SHALL constitute a protocol violation. Upon satisfaction of Crisis exit conditions, all Crisis-specific authorities, interpretations, and execution paths SHALL collapse immediately.

Delayed collapse, phased normalization, or post-hoc interpretive continuation of Crisis logic is forbidden.

---

10. Transparency and Audit

All Crisis actions MUST be:

- PTL-anchored,
- indexed by DTI-Day,
- cryptographically committed,
- publicly reviewable post-crisis under transparency, delay, and redaction rules defined by higher-layer audit protocols.

In states C3 and C4, the system SHALL initiate Final State Vector Broadcast, transmitting complete audit logs and system state snapshots to physically isolated external archives to preserve Physical Truth beyond system termination.

---

11. Finality Clause

Once frozen:

- any modification requires a new protocol identifier,
- mandatory full-system simulation under DKP-8-SIMULATION-001,
- explicit compatibility declaration.

Protocol Hash (SHA-256): [to be inserted at freeze]

END OF PROTOCOL

DKP-4-ERROR-001

Errors & Appeals Protocol

Version: 1.0

---

0. Preamble

DKP-4-ERROR-001 defines how the Dikenocracy system detects, corrects, and resolves **errors**, including erroneous actions, incorrect state transitions, and misapplied protocol outputs.

This protocol exists to ensure that Dikenocracy remains:

- self-correcting,
- reversible where possible,
- resistant to cascading failure,
- accountable without discretionary power.

Errors in DKP are treated as **system states**, not as moral failures or intent-based misconduct.

---

1. Purpose

The purpose of this protocol is to:

- provide a formal mechanism for identifying and correcting system errors,
- define appeal pathways for affected Subjects,
- prevent irreversible harm caused by incorrect execution,
- preserve trust in DKP through deterministic correction.

ERROR handling is strictly procedural and non-punitive.

---

2. System Position

This protocol operates:

- strictly downstream of DKP-0-ORACLE-001 (PTL) and DKP-0-TIME-001,
- downstream of DKP-1-IDENTITY-001, DKP-1-IMPACT-001, DKP-1-JUSTICE-001,
- downstream of all L3 protocols (INTERNAL-SEC, DEFENSE, ANTITERROR),
- upstream of DKP-4-CRISIS-001.

Hard constraints:

- DKP-4-ERROR-001 SHALL NOT introduce new coercive measures.
- DKP-4-ERROR-001 SHALL NOT reinterpret axioms or Physical Truth.
- DKP-4-ERROR-001 SHALL NOT override Justice outcomes, only request recomputation.

---

3. Core Definitions

3.1 Error

An Error is any PTL-confirmed deviation between:

- intended protocol behavior,
- actual system execution,
- or recorded system state,

where such deviation results in:

- incorrect restriction or action,
- incorrect attribution,
- incorrect impact calculation,
- incorrect application of protocol rules.

3.2 Appealable Decision

An Appealable Decision is any DKP action or outcome that:

- affects a Subject’s rights, access, assets, or status,
- is derived from protocol execution,
- is not explicitly marked as irreversible by higher-layer rules.

3.3 Appellant

An Appellant is any Subject who:

- is directly affected by an Appealable Decision, and
- submits a formal error claim under this protocol.

---

4. Error Classification

Errors are classified functionally:

- **E1 – Measurement Error**
  PTL sensor, data ingestion, or oracle misreporting.
- **E2 – Execution Error**
  Protocol logic executed incorrectly or out of order.
- **E3 – Attribution Error**
  Incorrect Identity binding or responsibility assignment.
- **E4 – Impact Computation Error**
  Incorrect impact magnitude, scope, or channel mapping.
- **E5 – Procedural Error**
  Violation of timing (DTI), escalation rules, or isolation constraints.

---

5. Error State Model (DTI-Governed)

- **R0 – No Error**
  - System operating within admissible parameters.
- **R1 – Error Suspected**
  - Error signal detected; non-coercive verification initiated.
- **R2 – Error Confirmed**
  - Error validated via PTL and protocol audit.
- **R3 – Correction Applied**
  - Corrective action executed.
- **R4 – Residual Dispute**
  - Correction completed, but appeal unresolved.

All states are indexed by DTI-Day and subject to timeouts.

---

6. Error Detection and Initiation

An error review MAY be initiated by:

- PTL-detected inconsistency,
- internal protocol audit,
- formal appeal submission by an Appellant accompanied by a minimal economic bond.

The bond SHALL be returned in full if the error is confirmed (R2). If the appeal is rejected as unfounded,
the bond SHALL be used to cover system audit costs.

No prediction or intent inference is permitted.

---

7. Appeal Submission

Appeals MUST:

- reference the specific Appealable Decision,
- include PTL-indexed evidence or pointers,
- be submitted within **30 DTI-Days** from the moment the decision was recorded in PTL,
- specify the alleged error category (E1–E5).

Errors of category **E1 (Oracle / Physical Truth error)** are not subject to any statute of limitations.

Upon formal validation of an appeal (state R1), execution of the contested decision, if reversible, MAY be temporarily suspended for up to **7 DTI-Days** (Status Quo Suspension) pending verification.

Appeals that do not meet formal requirements SHALL be rejected procedurally, without prejudice.

---

8. Review and Re-computation

Upon confirmation of an error:

- affected protocol outputs SHALL be recomputed,
- reversible effects SHALL be rolled back,
- irreversible effects SHALL be logged and compensated where possible,
- Justice MAY be re-invoked using corrected inputs.

ERROR handling never introduces new penalties.

---

9. Correction Principles

All corrections MUST:

- minimize secondary impact,
- preserve PTL consistency,
- prefer reversibility over compensation,
- avoid cascading changes outside the error scope.

If a **systemic or cascading error** is detected (impacting more than a protocol-defined threshold of Subjects
or cross-layer execution), DKP-4-ERROR-001 SHALL automatically escalate to DKP-4-CRISIS-001 for
Systemic Rollback and coordinated recovery.

---

10. Transparency and Audit

All error cases MUST be:

- logged with PTL anchoring,
- indexed by DTI-Day,
- reviewable post-factum,
- included in system reliability metrics.

---

11. Prohibited Actions

This protocol SHALL NOT:

- suppress valid appeals,
- retaliate against Appellants,
- hide error statistics,
- introduce discretionary overrides.

---

12. Finality Clause

Once frozen:

- modifications require a new protocol identifier,
- mandatory simulation under DKP-8-SIMULATION-001,
- explicit compatibility declaration.

Protocol Hash (SHA-256): [to be inserted at freeze]

END OF PROTOCOL

DKP-4-UPGRADE-001

System Upgrade & Anti-Capture Protocol

Version: 1.1
Status: Architecture Lock (Defense & Crisis Aligned)
Layer: L4 – Upgrade / Anti-Capture

---

0. Preamble

DKP-4-UPGRADE-001 defines the only lawful mechanism by which the Dikenocracy system may be modified after deployment.

In DKP, upgrades are treated as high-risk system events. Any change to formulas, thresholds, weights, or protocol logic may alter power balance, incentives, and survival guarantees.

This protocol exists to ensure that:

- system evolution remains possible,
- system capture remains impossible,
- no upgrade can bypass axioms, Physical Truth, Defense integrity, Crisis safeguards, or Justice constraints.

UPGRADE is not governance-by-vote; it is **governance-by-proof**.

---

1. Purpose

The purpose of this protocol is to:

- regulate changes to DKP formulas, parameters, and protocol logic,
- prevent hostile, covert, or incremental system capture,
- enforce full transparency, simulation, and reversibility of upgrades,
- provide deterministic rollback and recovery paths.

---

2. System Position

This protocol operates:

- strictly downstream of DKP-0-ORACLE-001 (PTL) and DKP-0-TIME-001,
- downstream of all L1–L3 execution protocols,
- downstream of DKP-4-ERROR-001 and DKP-4-CRISIS-001,
- upstream of DKP-8-SIMULATION-001 and DKP-8-AUDIT-001.

Hard constraints:

- DKP-4-UPGRADE-001 SHALL NOT redefine axioms (A1/A2).
- DKP-4-UPGRADE-001 SHALL NOT modify Physical Truth Layer rules.
- DKP-4-UPGRADE-001 SHALL NOT operate during active Crisis states (C1–C4).

Any modification of DKP-4-UPGRADE-001 itself SHALL require the highest security threshold and MUST demonstrably preserve or strengthen anti-capture guarantees relative to the current version.

---

3. Upgrade Definition

An Upgrade is any proposed change that affects:

- mathematical formulas, coefficients, or transformations,
- thresholds, weights, or scoring functions,
- protocol logic, state machines, or trigger conditions,
- cross-layer interactions or escalation rules.

Cosmetic, UI, documentation, or presentation changes are not considered upgrades under this protocol.

---

4. Upgrade Invariants (Hard)

4.1 Axiom Preservation

No upgrade SHALL weaken, reinterpret, or condition Axiom A1 (Preservation of Life) or Axiom A2 (Systemic Sustainability).

4.2 PTL Anchoring

All upgrade evaluation, validation, and acceptance MUST rely exclusively on PTL-verifiable data and simulations.

4.3 Non-Emergency Rule

Upgrades SHALL NOT be executed under urgency, fear, or crisis conditions.

4.4 No Silent Change

Every upgrade MUST be publicly visible, formally specified, and fully auditable.

4.5 Non-Degradation Invariant (Defense & Crisis)

No upgrade SHALL reduce, weaken, delay, condition, or probabilistically dilute the effectiveness, trigger sensitivity, execution scope, or response latency of:

- DKP-3-DEFENSE-001, or
- DKP-4-CRISIS-001

relative to the currently deployed version.

Any modification affecting L3 or L4 protocols MUST demonstrably preserve or strengthen survival guarantees under worst-case PTL-confirmed scenarios.

4.6 Physical Inevitability Preservation

Any upgrade affecting threat detection, Defense triggers, Crisis escalation logic, or containment boundaries MUST preserve the system's ability to respond to PTL-confirmed **Vectors of Physical Inevitability**.

Removal, weakening, probabilistic reinterpretation, or indirect delay of inevitability-based triggers is forbidden.

---

5. Upgrade Proposal Requirements

Any Upgrade Proposal MUST include:

- formal specification of all proposed changes,
- explicit before/after formula and logic comparison,
- expected Impact deltas across relevant domains,
- identified failure modes and deterministic rollback plan,

- full simulation parameters and assumptions.

Incomplete proposals SHALL be rejected procedurally.

---

6. Simulation and Proof Phase

Before approval, every upgrade MUST undergo:

- mandatory simulation under DKP-8-SIMULATION-001,
- stress-testing against adversarial and edge-case scenarios,
- capture-resistance analysis (including incremental takeover detection),
- public release of simulation results and methodology.

No simulation → no upgrade.

---

7. Anti-Capture Safeguards

The protocol SHALL enforce:

- caps on influence over upgrade initiation,
- detection of correlated proposals via DKP-1-IDENTITY-001 linkage,
- rejection of cumulative micro-upgrades converging toward capture,
- historical traceability of proposal lineage.

---

8. Approval and Activation

An upgrade MAY be activated only if:

- all simulations pass predefined safety and stability thresholds,
- no unresolved ERROR or Justice appeals remain,
- the activation window is publicly announced in advance.

Post-Crisis Cooldown Rule

Any upgrade affecting Defense, Crisis, Identity, or Justice layers SHALL NOT be proposed or activated until a full post-crisis audit and stabilization period has completed, as defined by DKP-8-AUDIT-001.

A mandatory Cooling-off Period SHALL apply:

- no less than **30 DTI-Days** MUST elapse between publication of final simulation results and activation.

During this period, any Subject MAY initiate DKP-4-ERROR-001 procedures upon detection of capture vectors, regressions, or hidden degradation.

Activation MUST:

- occur at a deterministic DTI-Day,
- be reversible within a defined window,
- be automatically logged and committed.

---

9. Rollback and Reversion

If post-activation monitoring detects:

- unexpected Impact deviation,
- instability or emergent capture vectors,
- violation of upgrade invariants,

then automatic rollback to the last stable version SHALL be triggered.

Critical errors SHALL NOT be corrected by stacking new upgrades on top of a faulty version.

Rollback priority is higher than optimization or feature progression.

---

10. Transparency and Audit

All upgrade-related artifacts MUST be:

- publicly accessible,
- PTL-anchored,
- permanently archived,
- auditable under DKP-8-AUDIT-001.

---

11. Prohibited Actions

This protocol SHALL NOT:

- allow emergency or crisis-time upgrades,
- permit opaque or discretionary parameter tuning,
- bypass simulation, audit, or cooling-off requirements,
- privilege specific Subjects, groups, or interests.

---

12. Finality Clause

Once frozen:

- any modification requires a new protocol identifier,
- mandatory simulation and audit,
- explicit compatibility declaration.

Protocol Hash (SHA-256): [to be inserted at freeze]

END OF PROTOCOL

DKP-5-CULTURE-001

Culture & Language Protocol

Version: 1.1
Status: Architecture Lock Candidate
Layer: L5 — Human Infrastructure
Anchored to: Genesis Block #0 (2025-12-10)

---

0. Preamble

DKP-5-CULTURE-001 defines culture and language as critical components of human cognitive infrastructure within Dikenocracy.

This protocol exists to preserve cultural plurality, linguistic diversity, and heterogeneous cognitive models, and to prevent systemic dominance of any single cultural, ideological, or semantic framework.

Culture within DKP is not treated as ideology, belief, or identity enforcement.

It is treated as a distributed cognitive environment that shapes interpretation, meaning-making, creativity, and social resilience.

This protocol explicitly rejects cultural optimization, convergence, homogenization, or ranking.

---

1. Purpose

The purpose of DKP-5-CULTURE-001 is to:

protect linguistic and cultural diversity as a system stability requirement,

prevent domination by a single cognitive or semantic model,

preserve minority and non-dominant cultural systems,

ensure cultural non-interference by governance algorithms,

decouple cultural expression from political legitimacy, economic advantage, or system trust.

This protocol does not define cultural values.
It defines hard boundaries against cultural suppression, capture, or instrumentalization.

---

2. System Position

DKP-5-CULTURE-001 operates:

Downstream of:

DKP-0-ORACLE-001 (Physical Truth Layer),

DKP-1-AXIOMS-001.

Parallel to:

DKP-5-EDU-001,

DKP-5-INFO-001.

Upstream of:

identity-neutral social and communicative interfaces.

Constrained by:

DKP-7-SCOPE-001,

DKP-8-SIMULATION-001.

This protocol SHALL NOT:

define belief systems or moral doctrines,

evaluate cultural content for correctness,

impose language hierarchies,

regulate personal identity or belief.

---

3. Definitions

Culture
A shared system of symbols, narratives, practices, and meaning-making structures transmitted socially rather than genetically.

Language
A structured symbolic system enabling communication, abstraction, and cognitive modeling.

Cognitive Model
A culturally influenced framework through which Subjects interpret reality, causality, and value.

Cultural Dominance
A condition in which a single culture, language, or cognitive model gains systemic advantage that suppresses alternative models.

Cultural Exception
A temporary, non-enforceable allowance granted to preserve cultural expression in conflict scenarios, without overriding higher-layer constraints.

---

4. Core Principles

4.1 Cultural Non-Domination

No culture, language, or cognitive model SHALL be granted systemic priority.

Governance algorithms MUST remain culture-neutral and language-agnostic.

No cultural framework may be treated as:

a default,

a baseline,

a reference model.

4.2 Linguistic Parity

All officially supported system interfaces SHALL be linguistically neutral.

Translation layers MUST:

preserve semantic fidelity,

preserve agency and intent,

avoid normative framing.

Lossy translation that alters meaning, agency, or intent constitutes a protocol violation.

4.3 Cultural Non-Optimization

Culture SHALL NOT be:

optimized,

ranked,

scored,

converged.

No metric may evaluate cultural “efficiency”, “progress”, or “superiority”.

Cultural persistence SHALL NOT be required to justify itself via:

economic performance,

demographic scale,

productivity metrics.

---

5. Prohibited Practices

The following are explicitly forbidden:

enforcement of cultural conformity,

suppression or marginalization of minority languages,

economic incentives tied to cultural assimilation,

algorithmic amplification of a dominant cultural narrative,

use of culture or language as a proxy for:

trust,

risk,

competence,

loyalty.

---

6. Protection of Minority and Non-Dominant Cultures

Minority cultures and languages SHALL be protected from:

systemic exclusion from public or system interfaces,

forced translation into dominant semantic frameworks,

erosion through algorithmic visibility bias.

Preservation mechanisms MAY include:

guaranteed interface availability,

archival and documentation support,

non-preferential access to infrastructure.

No preservation mechanism may:

impose behavioral obligations,

mandate participation,

require cultural self-identification.

---

7. Cultural Expression and Autonomy

Subjects retain full autonomy over cultural expression.

Participation in cultural systems SHALL be strictly voluntary.

No cultural affiliation SHALL affect:

legal status,

access to justice,

economic participation,

system privileges or obligations.

Cultural neutrality applies equally to dominant and minority cultures.

---

8. Interface Design Constraints

Human–system interfaces MUST:

avoid culturally loaded symbols by default,

support plural symbolic representations,

allow Subjects to select preferred linguistic and cultural contexts.

Default settings SHALL NOT encode:

cultural assumptions,

semantic hierarchies,

implicit normative frames.

---

9. Conflict and Override Rules

Cultural protection SHALL NOT override:

PTL-verified physical harm (DKP-0-ORACLE-001),

life-preservation constraints (DKP-1-AXIOMS-001),

scope and conflict rules (DKP-7-SCOPE-001).

In case of conflict with other L5 protocols:

a Cultural Exception MAY be declared,

such exception SHALL be:

temporary,

explicitly scoped,

non-enforceable,

logged for post-resolution audit.

Conflict resolution SHALL be governed by DKP-7-SCOPE-001.

Cultural or linguistic context SHALL NOT be used to:

exempt factual claims from verification under DKP-5-INFO-001,

block PTL-based safety or harm signals.

---

10. Audit and Transparency

Any algorithmic process interacting with cultural or linguistic content:

MUST be auditable for structural neutrality,

MUST expose bias-detection hooks,

MUST be reviewable post-facto.

Audits SHALL assess:

neutrality of structure and access,

absence of dominance amplification,

and SHALL NOT assess:

content value,

cultural merit,

ideological alignment.

---

11. Activation and Calibration Constraint

DKP-5-CULTURE-001 SHALL NOT introduce enforceable thresholds, rankings, or restrictions.

Any mechanism interacting with other protocols that may affect access or visibility:

MUST be simulated under DKP-8-SIMULATION-001,

MUST declare scope, duration, and reversibility,

MUST NOT create permanent cultural advantage or exclusion.

Absent valid L8 calibration, cultural interactions are informational and non-binding only.

---

12. Finality Clause

Once frozen:

this protocol is immutable,

any modification requires a new protocol identifier,

explicit compatibility declaration with DKP-7-SCOPE-001 is mandatory,

re-simulation of affected interfaces MAY be required.

Protocol Hash (SHA-256): [to be inserted at freeze]

DKP-5-EDU-001

Education Protocol

Version: 1.1
Status: Architecture Lock Candidate
Layer: L5 — Human Infrastructure
Anchored to: Genesis Block #0 (2025-12-10)

---

0. Preamble

DKP-5-EDU-001 defines education as a **core infrastructural component** of Dikenocracy, not as a cultural service, ideological instrument, or market good.

Education within DKP exists to ensure that all Subjects possess **sufficient cognitive and informational capacity** to:

- understand the system under which they operate,
- correctly interpret rights, obligations, and incentives,
- interact competently with algorithmic governance mechanisms,
- avoid systemic harm caused by ignorance, misinformation, or procedural misuse.

Education is treated as a **stability requirement**, not a value judgment and not a mechanism of social ranking.

---

1. Purpose

The purpose of DKP-5-EDU-001 is to:

- establish education as **mandatory cognitive infrastructure**,
- guarantee a **minimum system literacy capability set** for all Subjects,
- prevent governance asymmetry caused by informational inequality,
- decouple education from ideology, belief systems, or cultural conformity,
- anchor educational outcomes in **verifiable competence**, not credentials.

This protocol does **not** define culture, worldview, morality, intelligence, or personal values.

---

2. System Position

DKP-5-EDU-001 operates:

Downstream of:

- DKP-0-ORACLE-001 (Physical Truth Layer),
- DKP-0-TIME-001,
- DKP-1-AXIOMS-001,
- DKP-1-IDENTITY-001.

Upstream of:

- DKP-5-INFO-001,
- DKP-5-CULTURE-001.

Constrained by:

- DKP-7-SCOPE-001,
- DKP-8-SIMULATION-001.

Educational processes SHALL NOT influence:

- factual classification,
- verification outcomes,
- truth status under DKP-5-INFO-001.

This protocol SHALL NOT:

- impose ideological narratives,
- define moral or political correctness,
- evaluate beliefs, loyalties, or identities,
- restrict access to education based on opinion or worldview.

---

3. Definitions

Education
The structured acquisition of knowledge and skills necessary for competent interaction with physical reality and the DKP system.

System Literacy
A **capability set** enabling a Subject to understand DKP structure, rules, incentives, risks, and limits, and to act accordingly.

Competence
Demonstrable ability to apply knowledge correctly in defined contexts.

Educational Module
A bounded, verifiable unit of instruction targeting a specific competence domain.

Assessment Event
An auditable, reproducible process confirming competence through observable performance.

---

4. Core Principles

Education under DKP is governed by the following principles:

- **Comprehension over Memorization**
  Understanding system logic takes precedence over factual recall.

- **Competence over Credential**
  Diplomas, titles, or institutional affiliation carry no intrinsic authority.

- **Neutrality over Indoctrination**
  Educational content MUST remain free of ideological enforcement.

- **Accessibility over Exclusivity**
  Educational infrastructure MUST be universally accessible.

- **Verifiability over Authority**
  Educational outcomes MUST be auditable and reproducible.

---

5. Mandatory System Literacy Baseline

All Subjects interacting with DKP governance layers SHALL possess a **minimum system literacy capability set**.

The baseline capability set includes demonstrable competence in:

- DKP layer structure and protocol boundaries,
- individual rights and obligations,
- risk attribution and liability mechanics,
- dispute resolution and appeal pathways,
- scope limitations and exit rights.

Safeguards

Failure to meet baseline system literacy:

- SHALL NOT result in punishment,
- SHALL NOT result in permanent exclusion,
- SHALL NOT alter legal status or identity,
- MAY temporarily restrict access to **advanced or high-impact system functions**,
- MUST trigger **automatic, free educational remediation access**.

Education failures are **corrective signals**, not fault markers.

---

6. Educational Domains

DKP-recognized educational domains include:

- physical reality literacy (basic science, measurement, causality),
- system literacy (DKP architecture, protocols, and scope),
- economic literacy (resource flows, incentives, externalities),
- risk and safety literacy,
- digital and algorithmic literacy.

No domain SHALL:

- mandate belief acceptance,
- require worldview alignment,
- enforce cultural or moral conformity.

---

7. Assessment and Verification

Educational competence SHALL be verified through:

- standardized, open assessments,
- scenario-based evaluations,
- reproducible problem-solving tasks.

Assessments:

- MUST be transparent and auditable,
- MUST declare evaluation criteria,
- MUST minimize cultural and linguistic bias where possible,
- SHALL NOT evaluate ideology, belief, intent, or loyalty.

Assessment outcomes are **competence signals**, not judgments of worth or intelligence.

---

8. Adaptive Education and Remediation

When system interaction errors attributable to insufficient competence are detected:

- targeted educational modules MUST be offered,
- remediation SHALL prioritize assistance over restriction,
- repeated failure triggers **enhanced support**, not penalty.

Education functions as a **preventive stabilizer**, not an enforcement or disciplinary tool.

Permanent denial of access to education is **explicitly prohibited**.

---

9. Prohibited Practices

The following practices are explicitly forbidden:

- ideological indoctrination,

- political conditioning,
- loyalty testing or belief screening,
- punitive education models,
- credential-based privilege enforcement,
- substitution of education with economic or administrative penalties.

---

10. Transparency and Auditability

All educational content:

- MUST be open-source or publicly inspectable,
- MUST declare scope, objectives, and assessment criteria,
- MAY be audited under DKP-8-AUDIT-001.

Individual learning data:

- SHALL be minimized,
- SHALL be protected under DKP-7-SCOPE-001,
- SHALL NOT be repurposed for profiling or enforcement.

---

11. Scope Limitations

DKP-5-EDU-001 SHALL NOT:

- define personal success or intelligence,
- rank Subjects beyond competence requirements,
- enforce uniform educational paths,
- override cultural, religious, or personal identity,
- function as a gate for basic rights or dignity.

This protocol ensures **capability sufficiency**, not excellence or conformity.

---

12. Activation and Calibration Constraint

Any restriction of access to advanced system functions based on competence:

- MUST be defined as reversible,
- MUST be calibrated under DKP-8-SIMULATION-001,

- MUST include confidence bounds and review intervals.

Absent valid L8 calibration, educational signals are **informational only**.

---

13. Finality Clause

Once frozen:

- any modification requires a new protocol identifier,
- mandatory simulation under DKP-8-SIMULATION-001,
- explicit compatibility declaration with DKP-5-INFO-001 and DKP-7-SCOPE-001.

Protocol Hash (SHA-256): `[to be inserted at freeze]`

DKP-5-HABITAT-001

Living Space & Environmental Dignity Protocol

Version: 1.1
Status: Architecture Lock Candidate
Layer: L5 — Habitat
Anchored to: Genesis Block #0 (2025-12-10)

---

0. Preamble

DKP-5-HABITAT-001 defines the minimum physical standards of living space and environmental conditions under which Subjects exist within Dikenocracy.

This protocol treats habitat not as comfort, preference, or aesthetics, but as a matter of physical dignity.

Where DKP-5-TRANSPORT-001 protects dignity in motion, DKP-5-HABITAT-001 protects dignity in statics — the spatial and environmental conditions of everyday life.

This protocol exists to prevent:

physical degradation of living environments,

ghettoization through density and isolation,

biophysical stress as an invisible form of coercion,

erosion of human agency through hostile spatial design.

---

1. Purpose

The purpose of DKP-5-HABITAT-001 is to:

define a non-negotiable baseline of spatial dignity,

limit destructive population density and enclosure,

guarantee access to basic biospheric resources,

prevent long-term environmental harm to Subjects,

anchor habitat evaluation strictly in the Physical Truth Layer (PTL).

This protocol does not optimize urban form.
It establishes hard lower bounds below which habitat conditions are unacceptable.

---

2. System Position

DKP-5-HABITAT-001 operates:

Downstream of:

DKP-0-ORACLE-001 (Physical Truth Layer),

DKP-0-TIME-001,

DKP-1-AXIOMS-001,

DKP-2-FINANCE-001 (funding pathways only).

Upstream of:

DKP-5-INFO-001,

DKP-5-EDU-001,

DKP-5-CULTURE-001.

Constrained by:

DKP-7-SCOPE-001,

DKP-8-SIMULATION-001.

This protocol SHALL NOT:

define architectural styles,

impose cultural or aesthetic norms,

override local climatic or cultural adaptations,

activate enforcement without valid L8 calibration.

---

3. Definitions

Habitat
The physical environment in which a Subject resides for a sustained duration, including living space, immediate surroundings, and access paths to essential resources.

Living Space
An enclosed or semi-enclosed area intended for rest, shelter, and daily life.

Environmental Dignity
A state in which physical conditions do not impose chronic physiological stress beyond adaptive human capacity.

SPDI (Spatial Physical Dignity Index)
A composite, PTL-anchored physical index describing the adequacy of habitat conditions.

---

4. SPDI — Spatial Physical Dignity Index

SPDI is a normalized index in the range [0,1].

SPDI is derived exclusively from PTL-verified physical measurements, including but not limited to:

effective living space per Subject,

chronic ambient noise exposure,

access to natural light or circadian-supporting illumination,

air quality and ventilation adequacy,

thermal stability within survivable bounds,

access to clean water,

access to green or open space within a defined radius.

SPDI SHALL NOT incorporate:

subjective preference,

market value,

social or economic status indicators,

cultural or aesthetic metrics.

SPDI is a descriptive index, not a policy judgment.

---

5. Minimum Habitat Thresholds

A habitat is considered admissible only if all of the following hold:

SPDI ≥ SPDI_min,

no individual SPDI component falls below its critical survivability threshold,

chronic exposure parameters remain within PTL-confirmed safe limits.

Threshold Governance

SPDI_min and all component thresholds:

SHALL NOT be defined numerically within this protocol,

SHALL be specified, calibrated, and validated exclusively under DKP-8-SIMULATION-001,

SHALL be derived from biophysical research and PTL-confirmed survivability bounds,

SHALL NOT be lowered, overridden, or parameterized by economic, operational, or governance protocols.

---

6. Activation Gate (Mandatory)

DKP-5-HABITAT-001 is NON-ENFORCEABLE unless all of the following exist:

a valid L8 Calibration Bundle explicitly covering SPDI,

declared thresholds and confidence bounds,

a defined validity window,

an active linkage to DKP-8-AUDIT-001.

Absent a valid L8 bundle:

SPDI outputs are informational only,

no enforcement, restriction, or remediation may be triggered.

Manual interpretation of SPDI values is explicitly prohibited.

---

7. Density and Enclosure Constraints

Habitat design and allocation SHALL NOT:

exceed population density levels known to induce chronic biophysical stress,

create permanent enclosure without access to open environments,

rely on vertical compression as the primary solution to scarcity,

isolate populations from biospheric interaction.

Density and enclosure are evaluated indirectly via SPDI components, not via fixed architectural prescriptions.

---

8. Prohibited Conditions

The following constitute habitat violations:

persistent SPDI below minimum threshold,

deliberate creation of high-density containment zones,

denial of access to basic biospheric resources,

environmental degradation used as an economic or political lever,

spatial configurations designed to suppress autonomy or mobility.

Such conditions trigger mandatory remediation pathways.

---

9. PTL Anchoring and Verification

All SPDI measurements:

MUST be PTL-anchored,

MUST rely on physically verifiable data,

MUST be auditable and reproducible,

SHALL NOT depend on self-reporting alone.

Sensor tampering, suppression, or manipulation constitutes a critical integrity violation.

Detection, classification, and enforcement of sensor integrity violations are governed exclusively by:

DKP-0-ORACLE-001,

DKP-8-AUDIT-001.

DKP-5-HABITAT-001 SHALL NOT define independent investigative or punitive mechanisms.

—

10. Remediation and Compliance

When admissibility violations are confirmed:

remediation plans MUST be initiated,

relocation assistance MAY be provided,

economic incentives MAY be triggered via L2 protocols,

forced displacement SHALL NOT be used as a default remedy.

Persistent or systemic violations escalate to system-level review under DKP-7-SCOPE-001.

—

11. Scope Limitations

DKP-5-HABITAT-001 SHALL NOT:

rank habitats beyond minimum compliance,

enforce uniform living standards globally,

mandate specific housing forms,

override cultural or climatic adaptations.

This protocol enforces dignity floors, not optimization ceilings.

—

12. Transparency and Audit Hooks

SPDI values and violation flags:

MUST be available for audit,

MAY be aggregated to protect individual privacy,

SHALL be reviewable post-facto.

Individual-level exposure data SHALL be protected under DKP-7-SCOPE-001.

—

13. Finality Clause

Once frozen:

any modification requires a new protocol identifier,

mandatory simulation under DKP-8-SIMULATION-001,

explicit compatibility declaration with DKP-5-TRANSPORT-001 and DKP-7-SCOPE-001.

Protocol Hash (SHA-256): [to be inserted at freeze]

DKP-5-INFO-001

Information & Truth Protocol

Version: 1.1
Status: Architecture Lock Candidate
Layer: L5 — Information / Truth / Integrity
Anchored to: Genesis Block #0 (2025-12-10)

---

0. Preamble

DKP-5-INFO-001 defines how Dikenocracy handles information, factual truth, and systemic falsehood.

This protocol does not regulate opinions, beliefs, interpretations, or meanings.
It regulates verifiable factual claims and their systemic impact.

Where DKP-0-ORACLE-001 establishes Physical Truth, DKP-5-INFO-001 governs how informational acts interact with that truth.

This protocol exists to prevent:

systemic disinformation,

large-scale manipulation of perception,

erosion of Physical Truth through repetition of false claims,

weaponization of information against system stability.

Information governance under DKP is descriptive and non-coercive.

---

1. Purpose

The purpose of DKP-5-INFO-001 is to:

distinguish factual claims from opinion and interpretation,

define disinformation in PTL-anchored terms,

identify systemic lies as measurable system-level harm,

establish non-ideological informational responses,

preserve informational freedom without compromising Physical Truth.

This protocol does not seek consensus.
It seeks correspondence with reality.

---

2. System Position

DKP-5-INFO-001 operates:

Downstream of:

DKP-0-ORACLE-001 (Physical Truth Layer),

DKP-1-AXIOMS-001,

DKP-5-HABITAT-001,

DKP-5-TRANSPORT-001.

Upstream of:

DKP-5-EDU-001,

DKP-5-CULTURE-001.

Constrained by:

DKP-7-SCOPE-001,

DKP-8-SIMULATION-001.

This protocol SHALL NOT:

evaluate ideology, belief, or artistic expression,

enforce cognitive conformity,

mandate acceptance of verified claims,

activate enforcement without valid L8 calibration.

---

3. Definitions

Information Act
Any intentional transmission of a claim presented as factual.

Factual Claim
A statement asserting correspondence with physical reality and thus verifiable via PTL.

Opinion
A non-verifiable subjective position, interpretation, or value judgment.

Disinformation
The dissemination of factual claims demonstrably inconsistent with PTL-confirmed reality.

Systemic Lie
A persistent pattern of disinformation that measurably degrades system stability, safety, or Physical Truth coherence.

---

4. Classification of Information

Information acts are classified as:

I0 — Non-Factual Expression
Opinion, belief, satire, art, metaphor, speculation.

I1 — Unverified Claim
Factual claim pending PTL verification.

I2 — Verified Claim
PTL-consistent factual claim.

I3 — False Claim
PTL-inconsistent factual claim.

I4 — Systemic Disinformation
Persistent I3 with measurable systemic impact.

Only I2–I4 are subject to systemic evaluation.

---

5. Truth Determination

Truth status is determined exclusively by:

PTL outputs,

reproducible measurements,

cross-oracle consensus thresholds.

Truth SHALL NOT be determined by:

popularity,

authority,

repetition,

institutional endorsement,

social consensus.

Disputed claims remain I1 until PTL resolution or TTL expiry.

---

6. Temporal Resolution Rules (Mandatory)

To prevent indefinite suspension of unverified claims:

6.1 Temporal Transition

An I1 claim SHALL transition according to L8-calibrated temporal thresholds:

I1 + time ≤ T_1 → remains I1,

I1 + time > T_1 and PTL inconclusive → downgraded to informational annotation,

I1 + time > T_2 and PTL inconsistency emerges → reclassified as I3.

Values of T_1 and T_2 SHALL NOT be defined in this protocol and MUST be calibrated under DKP-8-SIMULATION-001.

6.2 Non-Blocking Rule

Unresolved I1 claims SHALL NOT:

block unrelated system operations,

suspend non-dependent protocols,

trigger enforcement.

I1 is informational unless escalated by PTL-confirmed impact.

---

7. Systemic Impact Assessment

A false claim escalates to Systemic Lie (I4) when:

repetition exceeds L8-calibrated propagation thresholds,

measurable harm to safety, infrastructure, or life occurs,

PTL coherence is degraded,

cascading misallocation of resources is triggered.

Impact assessment relies on:

PTL indicators,

downstream protocol disturbances,

measurable deviation from admissible system states.

---

8. Permitted Responses

Upon identification of I3 or I4 events, the system MAY:

attach PTL-anchored correction markers,

reduce algorithmic amplification of false claims,

trigger informational remediation channels,

flag systemic risk patterns for audit.

Informational Arbitration (Non-Removal Principle)

In the case of I4, the system SHALL NOT remove, erase, or delete informational records.

Instead, the system SHALL apply informational arbitration by annotation:

the original claim remains visible and preserved,

a PTL-anchored annotation is attached,

the annotation specifies:

nature of PTL inconsistency,

relevant oracle classes or node ranges,

quantified probability of correspondence with physical reality,

timestamped verification reference.

Annotations are informational disclosures, not enforcement actions.

Annotations SHALL NOT:

alter legal status,

impose penalties,

modify rights or obligations.

This mechanism:

preserves historical continuity for DKP-8-AUDIT-001,

prevents retroactive erasure of evidence,

prevents transformation of DKP into a censorship system.

The system SHALL NOT:

suppress opinions or beliefs,

enforce belief correction,

penalize individuals for isolated I3 events absent systemic impact.

---

9. Activation Gate (Mandatory)

DKP-5-INFO-001 is NON-ENFORCEABLE unless:

a valid L8 Calibration Bundle exists for:

propagation thresholds,

temporal transition parameters,

systemic impact metrics,

confidence bounds and validity windows are defined.

Absent a valid L8 bundle:

classifications above I1 are informational only,

no systemic remediation or escalation may be triggered.

Manual interpretation of truth status is explicitly prohibited.

---

10. Prohibited Actions

The system SHALL NOT:

criminalize false belief,

censor artistic or cultural expression,

mandate acceptance of verified claims,

perform psychological or ideological conditioning,

convert informational annotations into coercive enforcement.

Truth exposure is informational, not coercive.

---

11. Anti-Gaming and Abuse Prevention

Attempts to:

game verification thresholds,

exploit ambiguity to propagate falsehoods,

deliberately overload PTL with spurious claims,

manipulate propagation metrics,

are classified as systemic abuse and escalated to DKP-8-AUDIT-001.

---

12. Transparency and Verification

All truth classifications:

MUST be auditable,

MUST expose verification paths,

MAY be aggregated to protect privacy,

SHALL be reproducible by independent nodes.

Verification, not persuasion, is the basis of legitimacy.

---

13. Scope Limitations

DKP-5-INFO-001 SHALL NOT:

optimize narratives,

enforce social harmony,

resolve philosophical disputes,

adjudicate moral truth.

Its jurisdiction ends at factual correspondence with physical reality.

---

14. Finality Clause

Once frozen:

any modification requires a new protocol identifier,

mandatory simulation under DKP-8-SIMULATION-001,

explicit compatibility declaration with DKP-7-SCOPE-001.

Protocol Hash (SHA-256): [to be inserted at freeze]

DKP-5-TRANSPORT-001

Public Transport, Risk Reduction & Physical Dignity Protocol

Version: 0.2
Status: Draft (Integration Candidate)
Layer: L5 – Social Systems / Mobility

Depends on:

- DKP-0-ORACLE-001 (Physical Truth Layer)
- DKP-1-IDENTITY-001 (Identity & Subject Protocol)
- DKP-1-IMPACT-001 (Impact Measurement Protocol)
- DKP-2-ECONOMIC-001 (Economic & Externality Accounting)

---

1. Purpose

DKP-5-TRANSPORT-001 defines how a Dikenocratic system **designs, evaluates, and funds transportation infrastructure** in order to:

- minimize involuntary exposure to lethal physical risk,
- reduce systemic non-war mortality,
- preserve physical dignity of Subjects during mobility,
- shift behavioral equilibrium away from high-risk transport **without coercion or prohibition**.

Transportation safety is treated as a **system property**, not as an outcome of moral compliance or individual virtue.

This protocol does not regulate driving behavior directly.
It regulates **the physical and economic environment in which transport choices occur**.

---

2. Problem Statement: From Responsibility to Design

Empirical Physical Truth Layer data demonstrates that:

- private vehicle operation is one of the leading sources of non-war mortality,
- access to lethal transport mechanisms is granted after minimal qualification,
- public transport alternatives often impose physical degradation (crowding, forced standing, involuntary bodily contact),
- Subjects rationally choose higher-risk options when safer alternatives violate bodily dignity.

Therefore:

- road mortality is not primarily caused by irresponsibility,
- but by **design asymmetry between risk and physical comfort**.

Under Dikenocracy, such asymmetries are treated as **engineering defects**, not moral failures.

---

3. Core Principle

> **Safe modes of transport MUST be physically and psychologically preferable to dangerous ones.**

Safety that requires sacrifice of bodily dignity is not adopted at scale and SHALL NOT be assumed as a viable equilibrium.

---

4. Passenger Physical Dignity Index (PPDI)

The system SHALL compute, publish, and audit a mandatory metric:

PPDI — Passenger Physical Dignity Index

PPDI quantifies the physical conditions experienced by Subjects during transport.

4.1 PPDI Components (Non-Exhaustive)

PPDI SHALL include, at minimum, the following Physical Truth Layer–measurable indicators:

- percentage of trips completed **seated**,
- minimum guaranteed **individual seat width**,
- prohibition of **forced bodily contact** between non-consenting passengers,
- vibration and noise thresholds,
- thermal comfort range,
- average crowd density per cubic meter.

4.2 Classification

Transport modes operating below the minimum PPDI threshold are classified as:

Physically Degrading Transport Modes

This classification applies **regardless of cost efficiency or throughput**.

PPDI is a **system quality metric**, not a justice or liability score.

---

5. Standing Transport Reclassification

Standing transport is explicitly reclassified as follows:

- Standing passengers SHALL NOT be treated as a standard operating mode.
- Standing transport is permitted only under:
    - emergency conditions,
    - temporary overload events,
    - system recovery states.

If standing occurs **regularly**, the transport system SHALL be classified as:

Structurally under-provisioned

This classification triggers capacity expansion or logistical redesign, not passenger adaptation.

---

6. Vehicle Interior Architecture Constraints

Public transport vehicles SHALL prioritize:

- fully individual seating,
- spatial separation between passengers,
- staggered or chess-pattern layouts where applicable,
- elimination of continuous bench seating on core routes.

Loss of nominal capacity is acceptable where it results in:

- increased PPDI, and
- reduced dependency on high-risk private transport.

---

7. Risk Externalization Delta (RED)

7.1 Definition

Every kilometer traveled via private or high-risk transport modes generates measurable **probabilistic external harm**, including:

- mortality risk,
- medical system load,
- infrastructure degradation,
- systemic insurance exposure.

The Physical Truth Layer SHALL quantify this harm as:

RED — Risk Externalization Delta

7.2 Economic Treatment

RED is:

- computed via DKP-0-ORACLE-001 and DKP-1-IMPACT-001,
- recorded as an externality cost,
- redirected to fund high-PPDI transport infrastructure.

RED is **not a tax** and **not a punishment**.
It is deterministic damage compensation for probabilistic physical harm.

7.3 Identity-Weighted Risk Adjustment

RED computation MAY include **Identity-bound risk modulation** via DKP-1-IDENTITY-001, where:

- risk reduction is supported by PTL-confirmed data,
- Subjects with demonstrably lower impact profiles generate lower RED,
- no moral, reputational, or intent-based weighting is permitted.

This mechanism creates an economic incentive for skill, safety, and risk mitigation **without behavioral enforcement**.

---

8. Behavioral Equilibrium Shift

This protocol explicitly rejects:

- bans,
- moral pressure,
- punitive enforcement as primary tools.

Instead, it enforces a **comfort-driven equilibrium shift**:

When public transport becomes:

- seated,
- predictable,
- calm,
- physically dignified,

private high-risk transport demand declines organically, including among high-income Subjects.

---

9. Biophysical Impact Coupling

Transportation systems contribute materially to **biosphere state degradation**.

Therefore:

- transport-related impacts on biosphere indicators (B(t))
  SHALL be included in system evaluation,
- these impacts SHALL be measured via DKP-0-ORACLE-001,
- and SHALL influence funding, prioritization, and redesign decisions.

This coupling is **physical**, not ideological.

---

10. Success Criteria

The protocol is considered effective when:

- private vehicle kilometers decrease **without legal prohibition**,
- road mortality declines structurally, not episodically,
- PPDI scores trend upward year-over-year,

- public transport is voluntarily chosen across income strata,
- biospheric transport-related impact trends downward.

---

11. System Position

DKP-5-TRANSPORT-001 operates:

- downstream of Physical Truth (L0),
- downstream of Impact and Identity (L1),
- upstream of urban planning, labor mobility, and social systems,
- in coordination with economic externality accounting (L2).

This protocol SHALL NOT:

- assign justice outcomes,
- restrict individual freedoms,
- override Defense or Crisis protocols.

---

12. Protocol Status

This protocol did not previously exist as a unified DKP document.

What existed were:

- fragments,
- intuitions,
- moral arguments.

This document formalizes them as an **algorithmic infrastructure specification**.

Appendix A — Design Rationale & Safeguards (Normative)

A.1 Non-Overlap with Justice (L1)

Low PPDI or high RED SHALL NOT automatically trigger Justice outcomes.

They are treated as **system degradation signals**, not violations by Subjects.

Justice consequences may only arise through DKP-1-JUSTICE-001 using proper attribution and thresholds.

A.2 Non-Overlap with Defense (L3)

This protocol does not address active harm or hostile events.

Defense remains responsible for real-time containment of physical threats.

Transport redesign addresses **structural risk generation**, not attacks.

A.3 Autonomy & Future Transport Modes

Autonomous or assisted transport systems are evaluated identically:

- if RED approaches zero, economic pressure shifts to PPDI competition,
- ownership form is irrelevant,
- physical impact remains the sole criterion.

A.4 Axiom Compatibility

This protocol is compatible with:

- A1 (Preservation of Life),
- A5 (Externality Accountability),
- A7 (Minimum Suffering Constraint),

without encoding axioms as direct enforcement triggers.

A.5 Finality

Upon freeze:

- any modification requires a new protocol identifier,
- explicit incompatibility declaration,
- full-system simulation under DKP-8-SIMULATION.

END OF PROTOCOL

DKP-5-WORK-CYCLE-001

Work Cycle & Recovery Rhythm Protocol

Version: 0.3
Status: Draft (Architecture-stable)
Layer: L5 — Human Infrastructure

---

0. Preamble

DKP-5-WORK-CYCLE-001 defines the normative structure of work and recovery within Dikenocracy.

This protocol treats work cycles as a **physical, cognitive, and safety-critical infrastructure**, not as a cultural habit, moral expectation, or legacy industrial convention.
Human fatigue, error accumulation, and burnout are considered **systemic risks**, not individual failures.

Accordingly, the protocol abandons the culturally inherited 7-day week as a core unit and replaces it with a **physically neutral, mathematically exact, and biologically sustainable cycle**, fully compatible with DTI timekeeping.

---

1. Purpose

The purpose of DKP-5-WORK-CYCLE-001 is to:

- establish a deterministic, culture-neutral work/rest cycle,
- guarantee mandatory intra-day recovery,
- reduce systemic error, injury, and burnout risk,
- ensure compatibility with 24/7 critical infrastructure,
- decouple productivity from continuous human exhaustion,
- provide measurable constraints for workforce planning and simulation.

---

2. Scope

This protocol applies to:

- all standard labor arrangements under DKP,
- public services and private enterprises,
- critical and non-critical sectors.

Sector-specific adaptations are permitted **only if** all invariants defined herein are preserved.

---

3. Definitions

- **DTI-Day**
  A physical day indexed under DKP-0-TIME-001.
- **Cycle6**
  A 6-day overlay cycle defined as:
  `CycleDay = DTI-Day mod 6`
- **Workday (W)**
  A day containing a mandatory productive work obligation.
- **Restday (R)**
  A day containing no productive work obligation.
- **Presence Window**
  The total time a worker is scheduled to be available on a workday.
- **Productive Work Time**
  Time spent on direct labor tasks.
- **Recovery Block**
  Mandatory non-working time within a workday dedicated to recovery.

---

4. Standard Work Cycle

4.1 Cycle Structure

The normative default cycle is a **6-day cycle**:

```
[W, W, R, W, W, R]
```

Meaning:

- two consecutive workdays,
- one restday,
- two consecutive workdays,
- one restday.

4.2 Properties

- Maximum consecutive workdays: **2**
- Rest frequency: every **≤ 3 days**
- Full compatibility with a 360-day DTI year:
  - 360 / 6 = 60 exact cycles per year

The 7-day week is explicitly **non-normative** and may exist only as a local cultural overlay without legal or computational authority.

---

5. Daily Workday Structure

5.1 Normative Time Allocation (Workday)

Each workday SHALL be structured as follows:

- **Total Presence Window:** 10 hours
- **Productive Work Time:** 8 hours
- **Mandatory Recovery Block:** 2 hours

Formally:

Presence = 10h
Work = 8h
Recovery = 2h

5.2 Recommended Default Layout

A recommended (but not mandatory) structure:

- 4 hours productive work
- 2 hours recovery
- 4 hours productive work

5.3 Recovery Block Rules

- The recovery block:
    - is not counted as work time,
    - cannot be removed, reduced, or monetized,
    - does not require justification.
- Permitted recovery activities include:
    - meals,
    - sleep or rest,
    - personal or family needs,
    - non-work mobility.

The recovery block is considered **system-required**, not discretionary.

---

6. Cycle Accounting

Per 6-day cycle:

- Workdays: 4
- Restdays: 2
- Productive work: 32 hours
- Presence: 40 hours
- Recovery: 8 hours

Per DTI-Year (360 days):

- Workdays: 240
- Productive work: 1,920 hours
- Presence: 2,400 hours
- Mandatory recovery: 480 hours

---

7. Recovery Invariant (Hard Constraint)

Under no circumstances may a system-approved schedule violate the following invariant:

- No worker may be assigned more than **2 consecutive workdays** without a restday **OR**
- An equivalent, demonstrably safe recovery compensation must be provided.

Violation of this invariant constitutes a **system planning failure**, not individual misconduct.

---

8. 24/7 and High-Intensity Environments

8.1 Shift-Based Continuity

Continuous operation (e.g., hospitals, emergency services, infrastructure control) SHALL be achieved through:

- multiple shifts,
- workforce scaling,
- shift overlap,
- capacity buffering.

Continuous service SHALL NOT be achieved through exhaustion of individual workers.

8.2 Shift Requirements

Each shift SHALL preserve:

- a 10-hour presence window,
- 8 hours productive work,
- **minimum 2 hours recovery** per shift.

For high-intensity environments:

- **3–4 hours recovery per shift is recommended**, potentially fragmented.

8.3 Overlaps and Peak Load

- Overlapping shifts during peak hours are:
    - explicitly permitted,
    - treated as capacity design, not inefficiency.
- Simultaneous multi-shift presence during peaks is considered normal and encouraged.

---

9. Monitoring & KPIs (Minimum Set)

Implementations SHALL monitor at least:

- error and incident rates,
- sick leave frequency,
- staff attrition,
- output per productive hour,
- recovery compliance rate.

Persistent degradation in these metrics SHALL trigger mandatory schedule review.

---

10. Exceptions

Exceptions are permitted only:

- in clearly defined crisis scopes,
- for limited duration,
- with mandatory recovery compensation,
- and with full traceability under DKP crisis protocols.

No exception may establish precedent.

---

11. Architectural Principle

This protocol establishes a three-layer human time model:

1. **Productive Work**
2. **Mandatory Recovery**
3. **Full Rest**

Human recovery is treated as **infrastructure**, not as a personal optimization problem.

---

12. Summary Statement

DKP-5-WORK-CYCLE-001 replaces legacy industrial work rhythms with a mathematically exact, biologically sustainable, and governance-compatible cycle.

It ensures that:

- time is counted deterministically,
- recovery is guaranteed by design,
- productivity is stabilized through prevention of systemic harm,
- and continuous services are achieved through planning, not sacrifice.

DKP-6-EXIT-001

Exit Protocol

Version: 1.1
Status: Architecture Lock Candidate
Layer: L6 — Intersystem Level
Anchored to: Genesis Block #0 (2025-12-10)

---

0. Preamble

DKP-6-EXIT-001 formalizes the unconditional right of any Subject, region, or jurisdiction to exit the Dikenocracy system.

Exit is treated as a structural safety mechanism, not as defection, hostility, or failure.

This protocol exists to prevent coercive lock-in, systemic capture, and irreversible dependency.

No system claiming legitimacy may deny the right to leave.

Exit is a right.
System stability is a constraint, not a veto.

---

1. Purpose

The purpose of DKP-6-EXIT-001 is to:

ensure voluntary participation in Dikenocracy at all levels,

prevent enforcement through inescapability,

formalize exit consequences without punitive escalation,

guarantee reversibility of system membership,

protect overall system stability during disengagement.

Exit is not a sanction and not a failure signal.

---

2. System Position

DKP-6-EXIT-001 operates:

Downstream of:

DKP-1-IDENTITY-001,

DKP-2-FINANCE-001.

Parallel to:

DKP-6-INTEGRATION-001.

Upstream of:

DKP-4-CRISIS-001 (exit during crisis handling).

Constrained by:

DKP-7-SCOPE-001,

DKP-8-SIMULATION-001.

This protocol SHALL NOT:

prohibit exit under any circumstances,

criminalize exit decisions,

convert exit into a coercive tool,

permit indefinite suspension of exit rights.

---

3. Definitions

Exit
A formal termination of participation in DKP governance, execution, and incentive mechanisms.

Exiting Entity
An individual, organization, region, or jurisdiction initiating exit.

Exit Event
The time-indexed execution of exit following the declared procedure.

Cooling Period
A bounded, non-punitive delay between exit declaration and execution.

Restitution Tail
Residual obligations arising exclusively from verified past actions under DKP.

System-Critical Asset
An asset or dependency whose abrupt removal would cause measurable systemic instability.

---

4. Right to Exit

Any Subject or jurisdiction MAY initiate exit at any time.

Exit:

SHALL NOT require justification, approval, or vote,

SHALL NOT be blocked by economic status, political conflict, or crisis conditions,

SHALL NOT be revoked or suspended.

Exit becomes valid upon protocol-compliant declaration.

---

5. Exit Initiation

Exit initiation requires:

a cryptographically signed declaration of exit intent,

explicit declaration of exit scope:

individual,

organizational,

regional,

jurisdictional,

PTL-anchored timestamp.

No additional authorization is permitted.

---

6. Cooling Period and Exit Friction

Exit execution occurs after a fixed cooling period, calibrated exclusively under DKP-8-SIMULATION-001.

Purpose of Cooling Period

The cooling period exists to:

prevent cascading instability,

allow settlement of restitution tails,

enable orderly disengagement,

protect non-exiting parties from abrupt dependency loss.

Constraints

The cooling period:

SHALL be time-bounded,

SHALL NOT be indefinite,

SHALL NOT escalate obligations,

SHALL NOT restrict exit eligibility.

Cooling period parameters MAY vary by exit scope but MUST be declared, simulated, and auditable.

---

7. Phased Disengagement

Exit SHALL proceed through phased disengagement, not abrupt severance.

Phases MAY include:

governance disengagement,

enforcement disengagement,

financial settlement,

data separation.

The sequence and duration of phases MUST:

be declared at exit initiation,

be L8-simulated for stability,

preserve audit continuity.

---

8. Consequences of Exit

Upon completion of exit:

all future DKP obligations cease,

all future DKP benefits cease,

all governance, enforcement, and incentive mechanisms disengage.

Exit SHALL NOT:

annul historical responsibility,

erase impact records,

void verified restitution obligations.

---

9. Restitution Tail

Only verified liabilities incurred prior to exit declaration remain enforceable.

Restitution is limited to:

physically verified harm,

contractual obligations explicitly accepted under DKP,

unresolved impact costs measured before exit declaration.

Restitution SHALL NOT include:

ideological non-compliance,

punitive or exemplary damages,

hypothetical, projected, or speculative losses.

No new obligations may be generated after exit declaration.

---

10. System-Critical Assets and Delayed Settlement

If exit involves system-critical assets:

immediate severance MAY be delayed,

delayed settlement MUST be:

time-bounded,

compensated where applicable,

non-punitive,

transparently logged.

Delayed settlement SHALL NOT:

expand DKP authority,

create new obligations,

convert exit into forced participation.

---

11. Exit During Crisis

Exit during a declared crisis:

SHALL remain valid,

SHALL NOT be nullified or prohibited.

Temporary procedural adjustments MAY occur only to:

prevent immediate physical harm,

preserve minimal continuity for non-exiting parties.

Crisis handling:

SHALL NOT create exit precedent,

SHALL be strictly scoped under DKP-7-SCOPE-001,

SHALL NOT redefine exit rights.

---

12. Asset and Data Separation

Upon exit:

assets governed by DKP contracts are settled per DKP-2-FINANCE-001,

personal and operational data are frozen and archived,

no new data collection is permitted.

Data retention is limited to:

audit verification,

historical continuity,

restitution validation.

Post-exit data use for governance, profiling, or enforcement is prohibited.

---

13. Re-Entry

Exited entities MAY reapply under DKP-6-INTEGRATION-001.

Re-entry:

SHALL NOT be penalized,

SHALL NOT be delayed due to prior exit,

SHALL NOT treat exit history as disqualifying.

Outstanding restitution obligations MUST be resolved prior to re-entry.

---

14. Prohibited Practices

The following are explicitly forbidden:

denial or obstruction of exit rights,

collective punishment through exit,

retaliatory sanctions beyond restitution,

framing exit as treason, hostility, or illegitimacy,

exit-conditioned coercion, violence, or deprivation.

---

15. Scope Limitations

DKP-6-EXIT-001 SHALL NOT:

regulate non-DKP systems post-exit,

extend jurisdiction beyond the exit boundary,

interfere with sovereignty after disengagement.

DKP authority terminates at exit execution.

---

16. Finality Clause

Once frozen:

any modification requires a new protocol identifier,

mandatory simulation under DKP-8-SIMULATION-001,

explicit compatibility declaration with DKP-7-SCOPE-001.

Protocol Hash (SHA-256): [to be inserted at freeze]

DKP-6-INTEGRATION-001

Integration Protocol

Version: 1.1
Status: Architecture Lock Candidate
Layer: L6 — Intersystem Level
Anchored to: Genesis Block #0 (2025-12-10)

---

0. Preamble

DKP-6-INTEGRATION-001 defines the conditions, phases, and safeguards for onboarding countries, regions, cities, or sovereign jurisdictions into the Dikenocracy system.

Integration is designed to expand applicability without inducing economic shock, social destabilization, governance discontinuity, or Physical Truth degradation.

Integration is voluntary, controlled, phased, and reversible by design.
Participation in Dikenocracy is not compelled and not presumed.

This protocol exists to prevent:

financial or social collapse during onboarding,

forced convergence of legal or cultural systems,

import of unverified data or corrupted metrics,

expansion of DKP authority beyond validated scope.

Integration is not accession by decree.
It is a process of validated compatibility.

---

1. Purpose

The purpose of DKP-6-INTEGRATION-001 is to:

define a phased integration mechanism with explicit entry and exit criteria,

ensure continuity of Physical Truth and data integrity,

protect existing DKP participants from imported systemic risk,

protect integrating entities from abrupt protocol enforcement,

guarantee reversibility and rollback during early integration stages.

Integration success is defined by stable coexistence, not speed.

---

2. System Position

DKP-6-INTEGRATION-001 operates:

Downstream of:

DKP-0-ORACLE-001 (Physical Truth Layer),

DKP-1-AXIOMS-001,

DKP-7-SCOPE-001.

Upstream of:

DKP-6-EXIT-001,

all L5 sector protocols applied to new regions.

This protocol SHALL NOT:

force adoption of DKP,

override existing legal systems during transition,

impose cultural or ideological alignment,

expand DKP authority beyond the declared integration phase.

---

3. Definitions

Integrating Entity
A country, region, city, or jurisdiction applying to enter DKP.

Integration Phase
A bounded stage with explicitly defined rights, obligations, scope, and reversibility.

Shadow Mode
A non-enforcing observational state in which DKP ingests and analyzes data without producing legal, economic, or administrative effects.

Compatibility Metrics
PTL-anchored indicators used to assess readiness for phase progression.

Integration Shock
A measurable destabilization causally linked to DKP activation.

Rollback
A controlled reversion to a prior integration phase with declared scope and cost.

---

4. Core Principles

4.1 Voluntary Entry

No entity may be integrated without explicit, auditable consent.

Consent mechanisms MAY include:

referenda,

charter ratification,

legislative acts,

equivalent sovereign procedures.

Implicit or coerced consent is invalid.

4.2 Phased Integration

Integration SHALL occur through sequential phases.

No phase may be skipped.

No phase progression is automatic.

Each phase requires explicit entry and exit validation.

4.3 Reversibility

Early integration phases SHALL be fully reversible without punitive consequences.

Reversibility is a hard requirement until Full Integration is reached.

4.4 Scope Containment

During integration, DKP applicability SHALL be strictly limited to the declared phase scope.

No implicit extension of authority, enforcement, or dependency is permitted.

---

5. Integration Phases

5.1 Phase 0 — Observation (Shadow Mode)

Description
DKP systems ingest data in read-only mode.

Characteristics

No enforcement, incentives, or penalties,

No legal, economic, or administrative effects,

PTL compatibility and data quality assessment only.

Entry Conditions

Valid consent declaration,

PTL data access agreement.

Exit Conditions

Voluntary withdrawal, or

Successful completion of data integrity and coverage checks.

Notes Shadow Mode does not constitute compatibility proof.
It establishes observability only.

5.2 Phase 1 — Partial Interface

Description
Selected DKP modules MAY operate in advisory or opt-in mode.

Characteristics

No sanctions, kill switches, or automatic enforcement,

Local economic and legal systems remain fully sovereign.

Entry Conditions

Successful Phase 0 completion,

L8-simulated interface stability,

Declared scope of application.

Exit Conditions

Voluntary rollback to Phase 0, or

Verified operational stability within declared scope.

5.3 Phase 2 — Conditional Integration

Description
Defined DKP protocols become enforceable within limited domains.

Characteristics

Enforceability is scope-bound and time-bound,

Peace Staking and Physical Truth compliance MAY activate.

Entry Conditions

Successful Phase 1 completion,

DKP-8-SIMULATION-001 stress-test clearance,

Explicit declaration of enforceable domains.

Exit Conditions

Exit under DKP-6-EXIT-001 without punitive consequences,

Rollback to Phase 1 if shock indicators appear.

5.4 Phase 3 — Full Integration

Description
All applicable DKP protocols apply within declared scope.

Characteristics

Full rights and obligations are active,

Exit conditions transition to standard DKP-6-EXIT-001 rules.

Entry Conditions

Demonstrated long-term stability in Phase 2,

Absence of unresolved systemic risk,

Final consent reaffirmation.

---

6. Compatibility Assessment

Progression between phases requires verification of:

PTL data integrity and coverage,

absence of systemic manipulation,

minimum biosphere and safety thresholds,

administrative and technical capacity.

Assessment relies exclusively on:

PTL outputs,

reproducible metrics,

DKP-8-SIMULATION-001 stress testing.

---

7. Shock Prevention and Rollback

If Integration Shock indicators are detected:

phase progression SHALL halt automatically,

active enforcement SHALL be suspended,

rollback to the previous phase MAY be triggered.

Shock Indicators Include:

sudden welfare collapse,

financial instability beyond modeled bounds,

accelerated biospheric degradation,

systemic unrest causally linked to protocol activation.

Rollback Rules

rollback scope MUST be declared,

rollback costs MUST be logged,

rollback SHALL preserve data continuity and audit trails.

---

8. Protection of Existing Members

Integration SHALL NOT:

dilute existing protocol guarantees,

redistribute risk retroactively,

expose current members to imported instability.

Risk isolation and sandboxing SHALL be enforced during all non-final phases.

---

9. Cultural and Legal Non-Interference

During all integration phases:

local legal systems remain operative unless explicitly superseded,

cultural and linguistic systems remain untouched,

no harmonization is required beyond interface compatibility.

Cultural or legal divergence is not a failure condition.

---

10. Transparency and Auditability

All integration steps:

MUST be publicly documented,

MUST expose current phase, scope, and enforceability,

MAY be audited under DKP-8-AUDIT-001.

Audit focuses on process integrity, not political preference.

---

11. Prohibited Practices

The following are explicitly forbidden:

forced or accelerated integration,

conditional aid tied to DKP adoption,

retroactive enforcement,

use of integration to bypass DKP-7-SCOPE-001,

hidden dependency creation during early phases.

---

12. Finality Clause

Once frozen:

any modification requires a new protocol identifier,

mandatory simulation under DKP-8-SIMULATION-001,

explicit compatibility declaration with DKP-7-SCOPE-001.

Protocol Hash (SHA-256): [to be inserted at freeze]

DKP-7-PRIVACY-001
Data Privacy Protocol
Version: 1.0
Status: Draft
Layer: L7 — Meta / Scope / Transparency / Privacy

1. Preamble

   DKP-7-PRIVACY-001 defines privacy as a structural constraint of Dikenocracy, not as an individual privilege or moral claim.
   Privacy exists to prevent concentration of power through total visibility, to preserve subject autonomy, and to ensure that transparency mechanisms do not become instruments of coercion, surveillance, or behavioral control.
   This protocol does not negate transparency.
   It defines its hard limits.

2. Purpose

   The purpose of DKP-7-PRIVACY-001 is to:
   protect subjects from total observability,
   define which data may never be made public,
   formalize anonymity as a system invariant,
   prevent re-identification through data correlation,
   balance auditability with non-extractability of personal life.
   Privacy under DKP is a stability requirement, not a personal entitlement.

3. System Position

   DKP-7-PRIVACY-001 operates:
   parallel to DKP-7-SCOPE-001,
   parallel to DKP-7-TRANSPARENCY-001,
   downstream of DKP-1-AXIOMS-001,
   upstream of all audit, identity, and information protocols.
   This protocol constrains:
   DKP-7-TRANSPARENCY-001,
   DKP-8-AUDIT-001,
   DKP-5-INFO-001,
   DKP-5-EDU-001.
   No protocol may override privacy constraints except where explicitly permitted herein.

4. Definitions

   Personal Data — any data that can be causally linked to a specific Subject across time.
   Identifying Data — data that directly reveals subject identity.

Quasi-Identifying Data — data that enables re-identification via correlation.
Anonymous Data — data provably non-linkable to a Subject.
Privacy Breach — any condition enabling identity reconstruction beyond defined thresholds.

5. Core Privacy Principles

4.1 Non-Total Visibility
No Subject SHALL be fully observable across all system layers.
Total data aggregation across domains is forbidden.
4.2 Minimum Exposure
Only the minimum data required for protocol execution may be processed.
4.3 Non-Reidentification
The system MUST prevent identity reconstruction through data linkage.
4.4 Privacy over Convenience
Efficiency, optimization, or analytical value SHALL NOT justify privacy erosion.

6. Absolute Privacy Domains

The following domains SHALL ALWAYS remain private and non-public:
medical and biological data,
mental and psychological states,
intimate relationships,
beliefs, conscience, and inner conviction,
private communications not producing externalized impact.
These domains are non-extractable and non-auditable at the individual level.

7. Conditional Transparency Domains

The following MAY be exposed only in anonymized or aggregated form:
economic activity,
resource consumption,
mobility patterns,
educational interaction,
platform usage metrics.
Individual-level disclosure is forbidden unless explicitly triggered by higher-layer enforcement protocols within Scope.

8. Anonymity Guarantees

Subjects SHALL have the right to act anonymously wherever identity is not required for:
liability attribution,
risk allocation,
resource transfer.

Anonymous participation SHALL NOT reduce rights or access to system functions.

9. Audit Compatibility

   Audit processes:
   MUST operate on anonymized datasets where possible,
   MUST use zero-knowledge proofs for verification,
   SHALL NOT access raw personal data.
   Auditability applies to system behavior, not personal life.

10. Prohibited Practices

    The following are explicitly forbidden:
    mass surveillance,
    behavioral profiling,
    predictive policing,
    social credit scoring,
    cross-domain identity correlation.
    Violation constitutes a critical system integrity breach.

11. Crisis and Exception Handling

    Privacy SHALL NOT be suspended during crisis.
    Crisis protocols MAY:
    reduce anonymity only within explicitly bounded Crisis Scope,
    ONLY for direct life-preservation purposes.
    Any reduction:
    MUST be temporary,
    MUST be logged,
    MUST be reversible,
    SHALL NOT persist beyond Crisis Scope.

12. Transparency about Privacy

    All privacy rules, thresholds, and guarantees:
    MUST be public,
    MUST be auditable,
    MUST be verifiable by Subjects.
    Subjects must be able to verify what the system cannot see.

13. Scope Limitations

    DKP-7-PRIVACY-001 SHALL NOT:
    shield criminal liability,

prevent impact attribution,
override DKP-1-AXIOMS-001,
justify harm concealment.
Privacy is not immunity.

14. Finality Clause

Once frozen:
this protocol is immutable,
any modification requires a new protocol identifier,
mandatory simulation under DKP-8-SIMULATION-001,
explicit compatibility declaration with DKP-7-SCOPE-001 and
DKP-7-TRANSPARENCY-001.
Protocol Hash (SHA-256): [to be inserted at freeze]
END OF PROTOCOL

DKP-7-SCOPE-001

Scope & Limits Protocol

Version: 1.2
Status: Architecture Lock Candidate (Defense / Crisis / Upgrade Aligned)
Layer: L7 — Scope / Limits
Anchored to: Genesis Block #0 (2025-12-10)

---

0. Preamble

DKP-7-SCOPE-001 defines the strict applicability boundaries of the Dikenocracy system.

If L0–L4 describe how the system operates, DKP-7-SCOPE-001 defines where the system is allowed to operate — and where it is explicitly forbidden.

This protocol exists to prevent:

silent expansion of authority,

normalization of exceptional execution,

ideological, moral, or security-driven capture,

conversion of technical capability into implicit normative power.

Scope in DKP is not advisory.
It is a hard boundary layer.

Any protocol, execution logic, crisis mechanism, defensive action, or economic process operating outside the boundaries defined herein is invalid by definition, regardless of claimed benefit, efficiency, emergency justification, or net-positive utility.

---

1. Purpose

The purpose of DKP-7-SCOPE-001 is to:

define the maximal and minimal domains of DKP applicability,

prohibit algorithmic governance in domains where formalization causes irreversible harm,

constrain interpretation of axioms, Defense, and Crisis logic,

prevent exceptional execution from producing permanent authority,

guarantee exit, reversibility, and non-capture of the system.

This protocol does not optimize outcomes.
It limits power.

---

2. System Position

DKP-7-SCOPE-001 operates:

Downstream of:

DKP-0-ORACLE-001 (Physical Truth Layer),

DKP-1-AXIOMS-001.

Upstream of:

all L4–L6 protocols.

Binding constraint on:

DKP-3-DEFENSE-001,

DKP-4-CRISIS-001,

DKP-4-UPGRADE-001.

Validation boundary for:

DKP-8-SIMULATION-001,

DKP-8-AUDIT-001.

In case of conflict, DKP-7-SCOPE-001 prevails.

Absence of explicit permission in this protocol SHALL be interpreted as prohibition.

---

3. Scope Categories

System applicability is classified into four mutually exclusive domains.

S0 — Fully Applicable Domain

Algorithmic governance is permitted and enforceable.

Includes:

physical resource allocation under PTL constraints,

infrastructure coordination and safety execution,

economic settlement and accounting mechanisms,

identity continuity and audit logging,

non-discretionary execution of axioms.

S1 — Conditionally Applicable Domain

Algorithmic governance is permitted only under strict constraints.

Includes:

Defense execution under DKP-3-DEFENSE-001,

Crisis execution under DKP-4-CRISIS-001,

transitional degradation and recovery phases,

temporary suspension of non-essential functions,

emergency prioritization bounded by Axiom A1.

All S1 execution:

MUST be time-limited,

MUST be PTL-anchored,

MUST be auditable,

MUST degrade toward baseline (S0),

MUST NOT generate normative precedent.

Physical Inevitability Constraint

PTL-confirmed Vectors of Physical Inevitability MAY justify immediate defensive or crisis actions within S1, but SHALL NOT:

expand DKP applicability into new domains,

justify persistent S1 execution,

trigger automatic scope elevation beyond an explicitly declared Crisis Scope.

S2 — Restricted Domain

Algorithmic governance is partially prohibited.

Includes:

cultural expression and symbolic systems,

belief, ideology, religion, and worldview formation,

education beyond system literacy and verification rights,

artistic, linguistic, and meaning-making processes.

Within S2:

DKP MAY provide verification, factual grounding, and access to knowledge infrastructure,

DKP MUST provide tools for learning and validation,

DKP SHALL NOT define curricula or learning objectives,

DKP SHALL NOT rank, normalize, or optimize cultural or ideological content,

DKP SHALL NOT enforce behavioral or cognitive conformity.

S3 — Prohibited Domain

Algorithmic governance is explicitly forbidden.

Includes:

moral valuation or ranking of individual human lives,

utilitarian trade-offs of existence (“who should live”),

coercive belief shaping or ideological enforcement,

irreversible identity modification,

permanent suspension of exit rights,

formalization, optimization, ranking, enforcement, or algorithmic adjudication of private personal relationships, including friendship, love, family bonds, intimate relations, consent, and matters of conscience or faith,

creation of discretionary emergency authorities.

Any attempt to execute DKP logic within S3 constitutes a critical system violation.

---

4. Axiom Interpretation Constraint

Axioms define absolute boundaries.

Accordingly:

axioms SHALL NOT be interpreted by operational, economic, enforcement, Defense, Crisis, or optimization protocols,

axioms SHALL NOT be re-weighted, parameterized, or balanced against secondary objectives.

Interpretation of “minimum required conditions” under Axiom A1 is permitted only within an explicitly declared Crisis Scope.

For avoidance of doubt:

Crisis Scope is defined and activated only by DKP-4-CRISIS-001,

its permissible interpretation space is strictly bounded by DKP-7-SCOPE-001,

no other protocol may invoke, extend, simulate, or analogize “minimum required conditions” logic outside that bounded Crisis Scope.

Outside Crisis Scope:

axioms are executed, not interpreted.

---

5. Crisis Scope

Crisis Scope is a bounded sub-domain of S1.

Crisis Scope SHALL be entered only through the state machine and entry conditions of DKP-4-CRISIS-001.

Any attempt to enter Crisis Scope by inference, repetition, ambiguity, or downstream protocol logic constitutes a Scope violation.

Within Crisis Scope:

execution is survival-oriented,

authority is minimized,

reversibility has priority over optimization,

no permanent state change is permitted.

Crisis Scope explicitly forbids:

creation of new rights,

extension of authority duration,

modification of axioms,

generation of normative precedent,

implicit policy formation through repeated practice.

Post-Crisis Collapse Requirement

Upon PTL-confirmed satisfaction of DKP-4-CRISIS-001 exit conditions, Crisis Scope SHALL automatically collapse to S0.

Persistence of S1 execution beyond validated Crisis exit conditions constitutes a Scope violation.

---

6. Authority Decay Principle

Any temporary authority, elevated control surface, or exceptional execution path:

MUST be explicitly scoped,

MUST be time-bounded,

MUST decay over time,

MUST collapse to baseline execution upon stabilization.

No authority may be self-extending.

Persistence of authority requires:

renewed PTL-anchored justification,

mandatory validation under DKP-8-SIMULATION-001.

---

7. Defense Neutralization Boundary

Physical neutralization of a harm source performed under DKP-3-DEFENSE-001 or DKP-4-CRISIS-001:

SHALL be treated strictly as a physical harm-interruption action,

SHALL NOT expand DKP jurisdiction or applicability,

SHALL NOT convert the neutralized location, system, or territory into S0 or S1,

SHALL NOT create implicit governance, control, or normative authority.

Neutralization terminates harm.
It does not extend scope.

---

8. Non-Expansion and Anti-Gaslighting Safeguards

DKP execution SHALL NOT expand its scope by:

repeated crisis activation,

cumulative temporary measures,

statistical normalization of exceptions,

reinterpretation of edge cases,

omission, ambiguity, or silence.

Scope Escalation Safeguard

Any claimed divergence between PTL sensor outputs and observable physical reality, reported by a threshold number of Subjects, SHALL trigger a Scope Audit.

Such audit:

SHALL block transition from S0 to S1,

SHALL require confirmation by independent PTL nodes,

SHALL reject escalation based on single-sensor classes, isolated regions, or non-reproducible signals.

---

9. Exit and Non-Capture Guarantee

The right of exit is fundamental.

Accordingly:

exit SHALL NOT be conditioned on compliance,

exit SHALL NOT be delayed for optimization or stability goals,

exit SHALL NOT be suspended except temporarily within Crisis Scope to preserve immediate life.

Silent Exit Guarantee

The right of exit includes the right to receive a physically detachable equivalent of assets recorded under L2 protocols.

Such exit settlement:

SHALL NOT depend on continued DKP execution,

SHALL NOT require post-exit compliance,

SHALL be deliverable in non-protocol-bound form.

Economic friction SHALL NOT be used as a de facto restriction of exit.

Permanent restriction of exit constitutes system capture.

---

10. Transparency Boundary

Transparency obligations are scoped.

DKP guarantees:

access to verification mechanisms,

access to audit trails,

access to counterfactual and failure-mode simulations.

DKP does not guarantee:

human-readable explanation of internal models,

pedagogical simplification of algorithms,

normative justification beyond axiomatic execution.

Verification, not comprehension, is the basis of legitimacy.

---

11. Enforcement

Any execution exceeding the limits defined in DKP-7-SCOPE-001:

is invalid by definition,

MUST be flagged by audit systems,

MUST trigger containment and review.

Repeated violations constitute a critical system fault.

---

12. Finality Clause

DKP-7-SCOPE-001 is immutable once frozen.

Any modification requires:

a new protocol identifier,

mandatory simulation under DKP-8-SIMULATION-001,

explicit compatibility declaration across all dependent protocols.

Protocol Hash (SHA-256): [to be inserted at freeze]

DKP-7-TRANSPARENCY-001
Transparency Protocol
Version: 1.0
Status: Draft
Layer: L7 — System Integrity / Transparency

1. Preamble
   DKP-7-TRANSPARENCY-001 defines transparency as a structural integrity requirement of Dikenocracy.
   Transparency is not treated as radical openness, surveillance, or exposure of private life. It defines what MUST be public, what MUST remain anonymous, and how verification occurs without collapsing privacy or enabling coercion.
   This protocol exists to prevent:
   opaque governance,
   unverifiable power,
   identity-based coercion,
   false accountability through forced exposure.
2. Purpose
   The purpose of DKP-7-TRANSPARENCY-001 is to:
   ensure verifiability of system actions and outcomes,
   protect Subjects from surveillance or identity exposure,
   guarantee auditability without personal traceability,
   define strict separation between transparency and visibility,
   anchor legitimacy in verification, not disclosure.
3. System Position
   DKP-7-TRANSPARENCY-001 operates:
   downstream of DKP-0-ORACLE-001 (Physical Truth Layer),
   downstream of DKP-1-AXIOMS-001,
   downstream of DKP-7-SCOPE-001,
   upstream of DKP-8-AUDIT-001,

constraining all governance, economic, informational, and enforcement layers.
This protocol SHALL NOT:
mandate identity disclosure as a condition of participation,
expose private life, belief, or affiliation,
replace verification with reputation or popularity.

4. Core Distinctions
   Transparency — the ability to independently verify that a system action occurred and complied with protocol.
   Visibility — exposure of identity, personal data, or private behavior.
   Verification — cryptographic, physical, or procedural proof independent of trust in actors.
   Anonymity — the absence of linkability between a Subject and a specific action, except where explicitly required by higher axioms.
   Transparency SHALL NOT imply visibility.
5. Public-by-Default Domains
   The following system elements MUST be publicly transparent:
   protocol texts and versions,
   algorithmic logic and source code affecting governance,
   system-wide metrics and aggregate indicators,
   resource flows at institutional and protocol level,
   state transitions and execution traces.
   Public transparency applies at structural and aggregate levels only.
6. Protected-by-Default Domains
   The following domains MUST remain anonymous or privacy-protected:
   individual identity data,
   personal belief, opinion, or cultural affiliation,
   private communications,
   individual behavioral histories absent verified harm.
   No protocol may downgrade these protections without explicit Scope authorization.
7. Verification Without Identity
   Verification of actions SHALL rely on:
   cryptographic proofs,
   zero-knowledge attestations,
   PTL-anchored measurements,
   reproducible execution traces.
   Identity disclosure SHALL NOT be required unless:
   explicitly mandated by DKP-1-AXIOMS-001,
   or required to attribute verified harm under justice protocols.
8. Conditional De-Anonymization
   De-anonymization MAY occur only when:
   material harm is PTL-verified,
   causal attribution is required for restitution or containment,
   no anonymous remediation path exists.
   Any de-anonymization:
   MUST be minimal,

MUST be time-bound,
MUST be auditable,
SHALL NOT propagate beyond the specific case.

9. Prohibited Practices
   The following are explicitly forbidden:
   mass surveillance,
   identity-based scoring or profiling,
   forced transparency as punishment,
   linking unrelated datasets to infer identity,
   using transparency mechanisms for social control.
10. Transparency in Crisis and Exception
    During Crisis Scope activation:
    transparency of actions and decisions SHALL increase,
    identity exposure SHALL NOT increase by default.
    Emergency measures MUST be logged and reviewable post-facto.
    No crisis may justify permanent transparency expansion.
11. Interface Transparency
    Human–system interfaces MUST:
    explain why an action occurred,
    expose applicable protocol references,
    allow independent verification of outcomes,
    avoid persuasive or manipulative framing.
    Interfaces SHALL inform, not convince.
12. Audit Hooks
    All transparency mechanisms:
    MUST expose hooks for DKP-8-AUDIT-001,
    MUST preserve historical records,
    MAY aggregate data to protect privacy.
    Auditability SHALL NOT require identity exposure.
13. Scope Limitations
    DKP-7-TRANSPARENCY-001 SHALL NOT:
    define moral accountability,
    replace justice attribution,
    override cultural or informational protections,
    expand system scope.
    Transparency enforces verifiability, not control.
14. Finality Clause
    Once frozen:
    this protocol is immutable,
    any modification requires a new protocol identifier,
    mandatory compatibility declaration with DKP-7-SCOPE-001 and DKP-8-AUDIT-001.
    Protocol Hash (SHA-256): [to be inserted at freeze]
    END OF PROTOCOL

DKP-8-AUDIT-001
Continuous Audit Protocol
Version: 1.0
Status: Draft
Layer: L8 — Infrastructural Linkages / Integrity

1. Preamble
   DKP-8-AUDIT-001 defines the continuous, real-time audit framework of the Dikenocracy system.
   This protocol ensures that all protocol execution, data flows, parameter usage, and cross-layer interactions remain compliant with declared specifications, axioms, and scope limits.
   Audit in DKP is not retrospective inspection.
   It is a permanent structural condition of system operation.

Audit exists to:
detect protocol drift,
prevent silent capture or erosion of constraints,
expose unauthorized parameter influence,
ensure reproducibility of system behavior.

1. Purpose
   The purpose of DKP-8-AUDIT-001 is to:
   provide continuous verification of protocol compliance,
   ensure that all execution paths remain within declared bounds,
   detect deviations before they propagate into systemic harm,
   guarantee that no protocol operates outside its authorized scope,
   preserve trust through verifiable integrity rather than authority.

This protocol does not judge outcomes.
It verifies correctness of execution.

2. System Position
   DKP-8-AUDIT-001 operates:
   downstream of DKP-0-ORACLE-001 (Physical Truth Layer),
   downstream of DKP-8-SIMULATION-001,
   parallel to DKP-4-UPGRADE-001,
   upstream of enforcement, remediation, and halt mechanisms,
   constrained by DKP-7-SCOPE-001.

Audit outputs SHALL NOT:
override protocol logic,
introduce new rules,
modify parameters,
substitute for governance or justice decisions.

3. Definitions
   Audit Event — a verifiable record of protocol execution state.
   Audit Trace — an immutable sequence of Audit Events covering an execution interval.
   Audit Invariant — a condition that MUST hold true at all times.
   Deviation — any detected violation of protocol constraints, invariants, or declared interfaces.
   Silent Failure — deviation without explicit error or halt signal.
4. Audit Scope
   Continuous audit applies to:
   all protocol executions (L1–L8),
   all parameter accesses and updates,
   all oracle inputs and aggregation outputs,
   all cross-layer calls,
   all upgrade, crisis, and mercy invocations.

The following are explicitly excluded:
private beliefs,
non-system cultural expression,
off-chain activity without system effect.

5. Audit Invariants
   The following invariants MUST be continuously verified:

5.1 Axiom Compliance
No execution path SHALL violate DKP-1-AXIOMS-001.
Any detected axiom violation triggers immediate escalation.

5.2 Scope Compliance
No protocol SHALL operate outside its declared scope under DKP-7-SCOPE-001.
Scope expansion without formal upgrade constitutes a critical breach.

5.3 Parameter Integrity
No parameter MAY be modified outside DKP-4-UPGRADE-001.
Runtime tuning, adaptive optimization, or silent calibration are forbidden.

5.4 Determinism and Reproducibility
Given identical inputs, protocol execution MUST produce identical outputs.
Non-deterministic behavior constitutes an audit failure.

5.5 Attribution Integrity
All actions MUST remain traceable to valid Subjects per DKP-1-IDENTITY-001.
Loss of attribution is treated as systemic fault.

6. Audit Mechanisms
   Audit is implemented via:
   cryptographically signed execution traces,

state transition hashing,
cross-node replay verification,
independent recomputation by audit nodes,
continuous consistency checks across replicas.

Audit data MUST be:
immutable,
time-indexed,
publicly verifiable in aggregate,
selectively anonymized under DKP-7-SCOPE-001.

7. Deviation Classification
   Detected deviations are classified as:

D1 — Benign Anomaly (no systemic impact)
D2 — Constraint Violation (bounded, reversible)
D3 — Structural Breach (scope, axiom, or parameter integrity)
D4 — Capture Attempt (systematic, concealed, or coordinated)

Classification determines escalation pathway.

8. Response and Escalation
   Upon deviation detection:
   D1 events trigger logging and monitoring,
   D2 events trigger remediation protocols,
   D3 events trigger partial or full Systemic Halt,
   D4 events trigger immediate halt and mandatory upgrade review.

Audit SHALL NOT apply punishment.
Responses are procedural, not punitive.

9. Transparency and Access
   Audit outputs:
   MUST be accessible for independent verification,
   MAY be aggregated to protect individual privacy,
   SHALL expose methodology and invariants checked.

No audit process may be proprietary, closed, or authority-gated.

10. Non-Interference Principle
    Audit mechanisms SHALL NOT:
    modify live execution,
    inject corrective logic,
    mask failures,
    delay halt signals.

Audit observes and reports only.

11. Interaction with Crisis and Mercy
    During Crisis Mercy conditions:
    audit continues uninterrupted,
    all deviations remain recorded,
    no audit suspension is permitted.

Mercy affects response severity, not audit visibility.

12. Finality Clause
    Once frozen:
    this protocol is immutable,
    any modification requires a new protocol identifier,
    mandatory simulation under DKP-8-SIMULATION-001,
    explicit compatibility declaration with DKP-7-SCOPE-001.

Protocol Hash (SHA-256): [to be inserted at freeze]

END OF PROTOCOL

DKP-8-INTEROP-001

Interoperability Protocol
Version: 1.0
Status: Draft
Layer: L8 — Infrastructural Linkages

---

0. Preamble

DKP-8-INTEROP-001 defines how the Dikenocracy system interfaces with **external legal, economic, technical, and informational systems** that do not operate under DKP governance.

This protocol exists to ensure:

- compatibility without capture,
- interaction without authority leakage,
- exchange without normative contamination.

Interoperability under DKP is **translation, not submission**.

---

1. Purpose

The purpose of DKP-8-INTEROP-001 is to:

- define safe interaction boundaries with non-DKP systems,
- ensure deterministic translation between DKP and external regimes,
- prevent implicit authority transfer through integration layers,
- preserve DKP axioms, scope, and invariants under external coupling.

This protocol does NOT:

- harmonize legal systems,
- enforce DKP externally,
- accept external norms as binding within DKP.

---

2. System Position

DKP-8-INTEROP-001 operates:

- downstream of DKP-1-AXIOMS-001,
- downstream of DKP-7-SCOPE-001,
- downstream of DKP-8-SIMULATION-001,
- downstream of DKP-8-AUDIT-001,
- parallel to DKP-6-INTEGRATION-001 and DKP-6-EXIT-001.

This protocol is **purely translational**.

---

3. Definitions

External System — any legal, economic, technical, or informational system not governed by DKP protocols.

Interop Boundary — a formally defined interface where DKP state interacts with an external system.

Translation Layer — deterministic mapping between DKP-native representations and external representations.

Normative Leakage — implicit import of external authority, norms, or obligations into DKP without explicit protocol authorization.

---

4. Interoperability Invariants

4.1 **Axiomatic Supremacy**
No external system MAY override or reinterpret DKP axioms under any interoperability mechanism.

4.2 **Scope Preservation**
Interop SHALL NOT expand DKP jurisdiction beyond DKP-7-SCOPE-001.

4.3 **No Implicit Authority Transfer**
Technical or legal compatibility SHALL NOT be treated as legitimacy, obligation, or consent.

4.4 **Deterministic Translation Only**
All interoperability MUST operate via explicit, auditable translation rules.

---

5. Legal Interoperability

When interacting with external legal systems:

- DKP outputs MAY be exported as evidence, signals, or reference data,
- DKP SHALL NOT recognize external rulings as binding internally,
- legal compliance outside DKP is the responsibility of Subjects, not the system.

DKP does not adjudicate conflicts between external legal regimes.

---

6. Economic and Financial Interoperability

External economic systems MAY interact with DKP via:

- asset bridges,
- reporting gateways,
- settlement mirrors.

All external values MUST:

- be translated into justice-weighted internal equivalents,
- undergo full externality internalization,
- be flagged as externally sourced.

No external financial instrument may bypass DKP-2-FINANCE-001 constraints.

---

7. Technical Interoperability

Technical interoperability includes:

- data exchange,
- protocol bridges,
- API access,
- oracle mirroring.

Requirements:

- open specifications,
- cryptographic verifiability,

- audit hooks compatible with DKP-8-AUDIT-001.

Black-box or proprietary control logic SHALL NOT be trusted as authoritative inputs.

---

8. Informational Interoperability

External information MAY be ingested only as:

- untrusted inputs,
- I1 (Unverified Claims) under DKP-5-INFO-001.

External consensus, authority, or institutional validation SHALL NOT substitute PTL verification.

---

9. Failure and Degradation Modes

If an external system:

- becomes unreliable,
- violates invariants,
- attempts normative injection,

then:

- the interop boundary MUST degrade gracefully,
- DKP internal execution MUST remain unaffected,
- no rollback of DKP state is permitted.

Interop failure SHALL NOT trigger Crisis or Mercy mechanisms.

---

10. Prohibited Interoperability Patterns

Explicitly forbidden:

- automatic legal harmonization,
- algorithmic dependency on external decision systems,
- governance-by-API,
- silent import of external norms,
- permanent delegation of DKP functions.

---

11. Audit and Transparency

All interoperability layers:

- MUST be auditable,
- MUST expose translation logic,
- MUST record boundary events for post-facto review.

Audit authority is governed exclusively by DKP-8-AUDIT-001.

---

12. Scope Limitations

DKP-8-INTEROP-001 SHALL NOT:

- resolve geopolitical conflicts,
- unify legal systems,
- guarantee compliance by external actors,
- act as an enforcement bridge.

This protocol guarantees **compatibility, not convergence**.

---

13. Finality Clause

Once frozen:

- this protocol is immutable,
- any modification requires a new protocol identifier,
- mandatory simulation under DKP-8-SIMULATION-001,
- explicit compatibility declaration with DKP-7-SCOPE-001.

Protocol Hash (SHA-256): to be inserted at freeze

END OF PROTOCOL

DKP-8-SIMULATION-001

Simulation & Validation Protocol

Version: 1.1
Status: Architecture Lock Candidate
Layer: L8 — Simulation / Calibration / Validation

---

0. Preamble

DKP-8-SIMULATION-001 defines the exclusive and mandatory mechanisms by which proposed changes to the Dikenocracy system are tested, validated, calibrated, and stress-tested prior to any activation or deployment.

This protocol exists to ensure that no protocol, parameter, threshold, model, or external linkage is applied to the live system without prior verification against:

- **physical constraints (DKP-0-ORACLE-001),**
- **axiomatic invariants (DKP-1-AXIOMS-001),**
- **scope and conflict rules (DKP-7-SCOPE-001),**
- **systemic stability and reversibility requirements.**

Simulation under DKP is not forecasting, persuasion, or scenario storytelling.

Simulation is a deterministic falsification environment designed to reject unsafe or unstable changes.

---

1. Purpose

The purpose of DKP-8-SIMULATION-001 is to:

- **provide a mandatory pre-activation validation gate,**
- **calibrate all enforceable thresholds and composite indices,**
- **detect axiom and scope violations before execution,**
- **prevent irreversible harm caused by untested changes,**
- **ensure reproducible evaluation of protocol interactions,**
- **decouple experimentation from live system execution.**

Simulation is treated as a hard gate, not an advisory or optimization tool.

---

2. System Position

DKP-8-SIMULATION-001 operates:

Downstream of:

- **DKP-0-ORACLE-001 (Physical Truth Layer),**
- **DKP-1-AXIOMS-001,**
- **DKP-7-SCOPE-001.**

Upstream of:

- **all enforceable L5 protocols (HABITAT / INFO / EDU / CULTURE),**
- **DKP-6-INTEGRATION-001,**
- **DKP-6-EXIT-001,**
- **DKP-4-UPGRADE-001,**
- **DKP-8-AUDIT-001,**
- **DKP-8-INTEROP-001.**

Any protocol or change that introduces:

- **thresholds,**
- **activation conditions,**
- **composite indices,**
- **enforcement logic,**

- **calibration parameters,**
- **cross-layer dependencies,**

MUST pass DKP-8-SIMULATION-001 prior to activation.

No exception paths are permitted.

---

3. Definitions

Simulation Environment
An isolated execution space that mirrors DKP protocol logic without producing live effects.

Scenario
A bounded set of initial conditions, inputs, and constraints applied to the simulation.

Invariant
A condition derived from DKP-1-AXIOMS-001 and DKP-7-SCOPE-001 that MUST hold under all simulated states.

Failure State
Any simulated outcome that violates an invariant, exceeds declared risk envelopes, or produces irreversible harm.

Acceptance Criteria
Formal conditions that MUST be met for a change to be eligible for activation.

Calibration Bundle
A signed output artifact produced by L8 defining thresholds, models, confidence bounds, and validity windows.

---

4. Mandatory Simulation Scope

The following REQUIRE simulation and calibration under this protocol:

- **any DKP protocol modification or introduction,**
- **any parameter or threshold adjustment,**
- **any composite index definition (including B(t)),**
- **any enforcement or activation condition,**
- **any onboarding, exit, or integration mechanism,**
- **any interoperability with external systems.**

Protocols lacking an attached and valid L8 Calibration Bundle are NON-ENFORCEABLE by definition.

---

5. Simulation Inputs

Simulations MAY ingest:

- **historical PTL data,**
- **synthetic stress-test data,**
- **adversarial or worst-case inputs,**
- **boundary and failure-mode scenarios.**

Simulations SHALL NOT:

- **invent unphysical data,**
- **bypass PTL constraints,**
- **smooth, normalize, or cherry-pick inputs,**
- **optimize outcomes by selective sampling.**

All inputs MUST be:

- **explicitly declared,**
- **versioned,**
- **reproducible.**

---

6. Invariant Enforcement

During simulation, the following invariants MUST be enforced:

- **all axioms (DKP-1-AXIOMS-001),**
- **scope and conflict rules (DKP-7-SCOPE-001),**
- **life-preservation constraints,**
- **biosphere integrity constraints,**
- **non-expansion of authority,**
- **reversibility and rollback requirements.**

Violation of any invariant immediately invalidates the tested change.

---

7. Failure Classification

Simulation failures are classified as:

F1 — Hard Violation
Direct axiom or scope violation.

F2 — Systemic Instability
Runaway dynamics, cascading failures, deadlocks, or collapse conditions.

F3 — Irreversibility Breach
State transitions that cannot be rolled back within declared constraints.

F4 — Externality Leak
Unmeasured or displaced harm outside defined system boundaries.

Any F1–F3 failure blocks activation.
F4 requires explicit redesign and re-simulation.

---

8. Acceptance Criteria

A change is eligible for activation only if:

- **no invariant is violated,**
- **no F1–F3 failures occur,**
- **risk envelopes remain within declared bounds,**
- **behavior remains stable under adversarial scenarios,**
- **results are reproducible by independent nodes.**

Passing simulation does not mandate deployment.
It only permits eligibility.

---

9. Calibration & Output Contract (Mandatory)

Each successful simulation MUST produce a signed L8 Calibration Bundle containing:

- **defined thresholds,**
- **model specifications,**
- **aggregation logic,**
- **confidence bounds,**

- **validity window (time-bounded),**
- **applicable environmental or contextual assumptions.**

Composite Indices

Any composite index (including B(t)):

- **MUST have its model fully specified in L8,**
- **MUST declare all inputs and weights,**
- **MUST include uncertainty propagation,**
- **SHALL NOT be modified outside L8.**

PTL emits only raw, model-declared outputs.
Interpretation and calibration belong exclusively to L8.

---

10. Recalibration Triggers

A new simulation and calibration are REQUIRED upon:

- **environmental drift,**
- **social or behavioral regime change,**
- **technology or sensor class change,**
- **sustained audit divergence,**
- **protocol dependency update.**

Expired calibration bundles automatically invalidate enforcement.

---

11. Reproducibility and Transparency

All simulations MUST:

- **be deterministic given identical inputs,**
- **expose configuration, assumptions, and parameters,**
- **publish summary outcomes for audit,**
- **allow independent re-execution.**

Simulation artifacts MAY be anonymized but SHALL NOT be opaque.

---

12. Non-Override Rule

Simulation outcomes SHALL NOT be overridden by:

- **political discretion,**
- **economic pressure,**
- **emergency rationale,**
- **human authority.**

Failure in simulation cannot be appealed.
Only redesign and re-simulation are permitted.

---

13. Relationship to Audit

DKP-8-AUDIT-001 SHALL:

- **verify deployed behavior against simulated behavior,**
- **flag divergence beyond tolerance,**
- **trigger rollback or halt when required.**

Simulation defines the reference reality for audit comparison.

---

14. Finality Clause

Once frozen:

- **this protocol is immutable,**
- **any modification requires a new protocol identifier,**
- **explicit incompatibility declaration is mandatory,**
- **full re-simulation of all dependent protocols is required.**

Protocol Hash (SHA-256): `[to be inserted at freeze]`