

NOVAK Laws L0–L15 — Core Protocol Specification

Authoritative Cryptographic Governance Framework for Proof-Before-Action Systems

Abstract

The NOVAK Protocol establishes a deterministic proof-before-action model for all computational systems, ensuring no action occurs unless cryptographic integrity is mathematically verified.

These laws define the **execution boundaries**, **cryptographic identities**, **decision gates**, and **audit-chain rules** for any system implementing the NOVAK model.

These laws must be included **unaltered** in every implementation, documentation set, or regulated deployment.

They serve as the non-negotiable baseline of the NOVAK Execution Integrity Standard.

0. Overview of NOVAK Execution Integrity

Traditional systems act on data first and audit later.

NOVAK reverses this:

NOVAK requires mathematical proof *before* any action is allowed.

No cryptographic proof → No execution.

This ensures:

- No silent corruption
- No tampering-drift
- No unauthorized code paths
- No unverifiable decisions
- Tamper visibility across all steps

The NOVAK Laws L0–L15 codify the enforcement structure.

L0 — The Zeroth Law (Prime Directive of NOVAK)

No system may act unless cryptographic proof confirms the input, rules, and output have not changed.

This is the foundation.

Every other NOVAK law is subordinate to L0.

L1 — Deterministic Rule Execution

Every computation must produce the same output for the same inputs, rules, and environment.
Non-determinism is forbidden unless explicitly declared.

L2 — Rule Hash (HR)

Each regulatory, procedural, or logical rule applied must have a unique cryptographic identity:

$$\text{HR} = \text{Hash}(\text{Rule Definition})$$

Rules cannot be executed unless their HR matches the approved version.

L3 — Data Hash (HD)

All decision-making data must be hashed before use:

$$\text{HD} = \text{Hash(Data)}$$

Tampered, incomplete, or altered data immediately invalidates execution.

L4 — Output Hash (HO)

The output of the computation must be hashed:

$$HO = \text{Hash}(Output)$$

HO must match the expected digest before the output is allowed to be used.

L5 — Execution Binding (HVET)

NOVAK binds rule, data, and output into a single immutable identity:

$$\text{HVET} = \text{Hash}(\text{HR} + \text{HD} + \text{HO})$$

This cryptographic object is the “execution identity receipt.”

L6 — HVET Must Precede Action

No action can occur unless:

Provided HVET == Expected HVET

If mismatch:

- **Execution halts**
- **Output invalidated**
- **Chain integrity alarm triggered**

L7 — Frozen Snapshot Requirement

All NOVAK decisions must reference a frozen snapshot of inputs.

Live data streams cannot be trusted until hashed and frozen.

L8 — Recursive Global Audit Chain (RGAC)

NOVAK requires every approved HVET become the next link:

$\text{Receipt}(n) = \text{Hash}(\text{Receipt}(n-1) + \text{HVET}(n))$

This forms an unstoppable, self-verifying audit ledger without needing blockchain.

L9 — Forward-Only Integrity

NOVAK prohibits:

- rewriting history
- erasing links
- selective rollback
- partial execution

Every drift must be visible.

L10 — Zero Trust Execution Model

The system must assume:

- data can lie
- rules can drift
- outputs can be corrupted
- memory can be manipulated

Only cryptography determines trust.

L11 — No Hidden States

All inputs, rules, and outputs must be explicitly included in HR, HD, HO, and HVET.
No undocumented variables.

L12 — Deterministic Safety Gate (formerly HARMONEE- Original Name)

This is the enforcement layer that blocks execution until HVET validation succeeds.

It must be:

- deterministic
- non-bypassable
- visible
- measurable
- cryptographically enforced

L13 — Global Verifier Canon (formerly REVELATION - Original Name)

All verification logic must be publicly documentable and independently auditably re-runnable.

If the verifier cannot be rerun → the action cannot be trusted → the system is non-NOVAK-compliant.

L14 — Identity Receipt (formerly NIPS - Original Name)

Every action must produce an EIR:

EIR = { HR, HD, HO, HVET, Timestamp, Actor }

This becomes authoritative proof of state.

L15 — Full Disclosure Rule

Any system claiming NOVAK compliance must disclose:

- all recording rules
- hashing mechanisms
- failure modes
- chain linkages
- audit logic
- HVET structure
- allowed hash families

No black boxes.

Conclusion

These fifteen laws define the universal mathematical governance model of NOVAK. Any system—governmental, financial, medical, robotic, or AI—can adopt these laws to guarantee the highest level of integrity, accountability, and cryptographic certainty before action.