# THE NOVAK PROTOCOL — OFFICIAL PUBLIC SPECIFICATION

**Version:** 1.0
**First Published:** 10 November 2025
**Author:** *Matthew S. Novak*
**Protocol Name: N.O.V.A.K — Novak Objective Verification of Autonomous Knowledge**
**Status:** Public reference design, open for cryptographic challenge
**License:** NOVAK-PUBLIC / NOVAK-COMMERCIAL (dual license)

---

## 🔷 1. Executive Summary

NOVAK is the first computational execution-governance model that **mathematically prevents unlawful machine or institutional decisions** by requiring cryptographic proof of legal compliance *before* execution occurs.

Unlike audit logs, compliance checklists, or blockchain immutability — all of which allow illegal behavior to occur and be analyzed later — NOVAK **stops unlawful execution at runtime**, making silent institutional wrongdoing *mathematically impossible.*

NOVAK consists of four enforcement primitives:

1. **NIPS** — Novak Input Proof Set
   *No unverifiable input is permitted.*

2. **HARMONEE** — Hash-Attested Receipt of Machine Output, Non-Repudiable, Enforceable & Eternal
   *Every execution produces an immutable receipt.*

3. **REVELATION** — Recursive Execution Ledger Validator for All Transactions In Ordered Number
   *All receipts are chained so deletion becomes forensic evidence.*

4. **Equal Execution Law** —
   *Identical inputs under identical rules MUST yield identical outputs — OR must generate human-readable justification.*

These four components comprise the **NOVAK Kernel**, the first enforceable digital rule-of-law mechanism for autonomous systems.

---

# 🔷 2. The Five Novak Laws of Cryptographic Execution Integrity

**LAW 1 — VERIFIED INPUT ONLY**
 No system may execute using inputs which cannot prove cryptographic origin, schema validity, and provenance.

**LAW 2 — IMMUTABLE EXECUTION RECEIPTS**
 Every execution MUST produce a cryptographically bound proof containing rule, input, output, actor, timestamp.

**LAW 3 — GLOBAL AUDIT CONSISTENCY**
 Receipts MUST chain into a recursive hash ledger so deletion or mutation becomes automatically detectable.

**LAW 4 — EQUAL EXECUTION REQUIREMENT**
 Identical rule + input pairs MUST produce identical outputs OR a justification-proof must be generated.

**LAW 5 — PUBLIC VERIFIABILITY**
 Any third party must be able to validate execution integrity using public cryptographic material without trusting the institution itself.

---

# 🔷 3. Formal Mathematical Specification

### 3.1 Deterministic Decision Function

```
O = f(R, D)
```

Where:

- $R$ = Frozen rule bundle hash

- $D$ = Attested input bundle

- O = Output state

---

## 3.2 NOVAK Execution Receipt (HARMONEE)

```
H = Hash(R_H // D_H // O_H // Actor_ID // Timestamp)
```

---

## 3.3 REVELATION Global Ledger Chain

```
C₀ = GENESIS
C  = SHA256(C ₋₁ // H )
```

Any mutation → C□ ≠ recomputed C□ → forensic proof of tampering

---

## 3.4 NOVAK Equal Execution Law

```
IF
  R(D₁) → O₁
  R(D₂) → O₂
AND
  D₁ ≡ D₂  (materially equivalent)
AND
  O₁ ≠ O₂
THEN
  System MUST produce justification J
IF J = NULL → EXECUTION VIOLATION
```
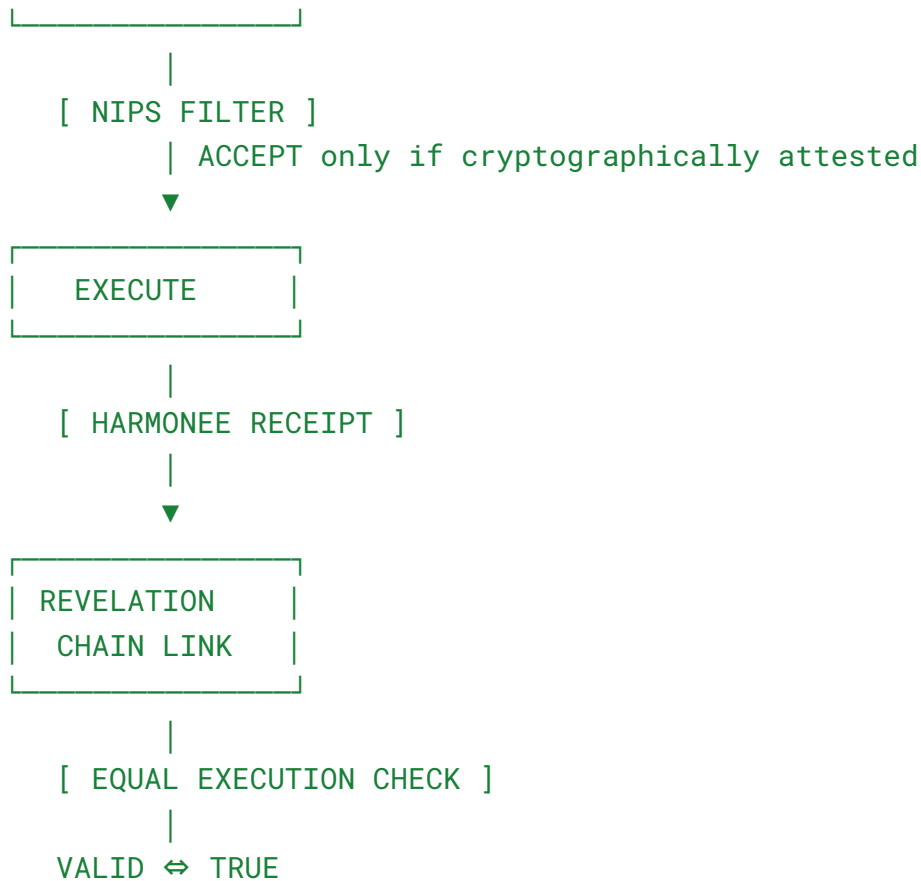
This is **the first enforceable mathematical definition of lawful equality under algorithmic governance.**

---

# 🔷 4. NOVAK Kernel Enforcement Flow

```
        ┌─────────────┐
        │    INPUT     │
```

```
└───────────────┘
                |
       [ NIPS FILTER ]
              | ACCEPT only if cryptographically attested
              ▼
       ┌───────────────┐
       │   EXECUTE     │
       └───────────────┘
              |
       [ HARMONEE RECEIPT ]
              |
              ▼
       ┌───────────────┐
       │ REVELATION    │
       │  CHAIN LINK   │
       └───────────────┘
              |
       [ EQUAL EXECUTION CHECK ]
              |
         VALID ⇔ TRUE
```

---

## 🔷 5. NOVAK Licensing Model

✔ **Free, unrestricted use for U.S. federal agencies**

✔ **Commercial license required for any profit-seeking deployment**

✔ **NOVAK-PUBLIC License** for research, academia, open audits

✔ **NOVAK-COMMERCIAL License** for enterprise full deployment

---

## 🔷 6. NOVAK Authoritative Reference Text

**This document SHALL be referenced as:**

*"NOVAK v1.0 — Public Enforcement Specification Release (10 November 2025)"*

---

# 🔷 7. Cryptographic Challenge Rules

Anyone may:

- ✔ attempt to break deterministic equality
- ✔ attempt to produce unverifiable inputs
- ✔ attempt to alter receipts undetected

If successful, they MUST:

- ➡ publish the exploit
- ➡ submit reproduction steps
- ➡ receive authorship credit

If NO ONE breaks it → **the system becomes canon by survival.**

---

# 🔷 8. Author Declaration

I, **Matthew S. Novak**, hereby publish the NOVAK Protocol into the public scientific record, retaining authorship and commercial rights while granting unrestricted U.S. government use.

First published, timestamped, and archived: **10 November 2025**