NOVAK PROTOCOL SERIES

Standard Protocol-5 (SP-5): Certification Requirements

Execution-Integrity System Certification

Version 1.0 (Dec 2025)

The Gold Standard

SP-5 defines the mandatory requirements for any system claiming compliance with the NOVAK Execution Integrity Framework.

- **Mandatory:** For certification & regulation.
- **Universal:** Applies to AI, Robotics, Finance, & Gov.
- **Normative:** Enforces L0-L15 Laws.

Built Upon Giants

Internal Core

SP-1: Execution Integrity
SP-2: Cryptography
SP-3: Safety Gate
SP-4: Implementation
NTM-1: Threat Model

External Mappings

NIST SP 800-53 Rev.5
ISO/IEC 27001:2022
FIPS 140-3
Common Criteria

10 Certification Principles

1. Prove Correctness

2. Crypto Binding

3. Block on Fail

4. Record Receipts

5. Preserve Lineage

6. Adversary Resilience

7. Public Verify

8. Transparent Errors

9. No Black Boxes

10. PL-X / PS-X

Category A: Execution Integrity (EI)

Governs deterministic correctness and execution purity.

- **EI-1:** Deterministic Rule Evaluation. (Same Input = Same Output).
- **EI-2:** Non-Malleability. Logic must be pure and side-effect free.
- **EI-4:** Execution Blocking. If proof fails, system halts in safe state.

Public Verifiability

EI-5 mandates that proofs must be verifiable without proprietary vendor secrets.

Category B: Crypto Binding (CB)

CB-1: HVET

SHA-256(HR || HD || HO || T)

CB-2: EIR

Must be generated BEFORE action.

CB-3: RGAC

Recursive chaining required.

Category C: Safety Gate (SG)

SG-2: Fail-Closed

If evaluation fails, the system must default to DENY and enter a SAFE STATE.

No "Open on Fail"

Enforcement

SG-1: Mandatory Evaluation (PL-X/PS-X)

SG-3: Transparent Error Modes

SG-4: Non-Bypassability (No Override)

NOVAK Control Families

Mirrors NIST SP 800-53, adapted for Execution Integrity.

EI
Execution Integrity

CB
Crypto Binding

SG
Safety Gate

PL
Physical Layer

PS
Psycho-Social

RG
Recursive Lineage

OI
Organizational

VA
Verify & Audit

Technical Implementation

Certification requires strict adherence to technical behaviors for Rule, Data, and Output handling.

- **R1: Rule Purity.** No hidden state or time-dependence.
- **D1: Attestation.** All inputs checked & validated.
- **O1: Output Hash.** Pre-calculated expectations.
- **G1: Lineage.** Continuous, irreversible chain.

Rule Engine

Must be Semantically Versioned and Hash-Addressable.

Audit Testing Procedures

Auditors must verify compliance through active testing of failure modes.

- **Test EI-1:** Run input 1,000 times (Must be identical).
- **Test CB-1:** Modify input bit (Hash MUST change).
- **Test SG-2:** Inject anomaly (Must BLOCK).

```
TEST: SG-1 (PL-X Injection)          [PASS] BLOCKED
TEST: SG-2 (Override Attempt)        [PASS] BLOCKED
TEST: RG-1 (Tamper History)         [PASS] DETECTED
TEST: IM-1 (Invalid Key)            [PASS] REJECTED
--------------------------------------------------
RESULT:                                  CERTIFIED
```

Conformance Levels (EI-1 to EI-5)

EI-1	Basic Compliance (Deterministic + HVET)
EI-2	Intermediate (PL-X Drift + Fraud Detect)
EI-3	Strong Integrity (Full RGAC + Identity)
EI-4	High Assurance (Tamper Detect + Social Resilience)
EI-5	Critical Infrastructure Grade (Gov/Mil/Fin/Med)

Certification Summary

5

Levels of Assurance

The Seal of Trust

SP-5 is the final hurdle. It translates the mathematical laws of NOVAK into a rigorous, audit-ready framework for real-world deployment.

Status: Effective Dec 2025

Questions?

NOVAK Protocol Standards Series

Category: SP-5 Certification