📘 SP-5 — NOVAK CERTIFICATION STANDARD

NOVAK Series Standard SP-5
Execution-Integrity System Certification Requirements

Version: 1.0
Status: Draft for Public Review
Issued by: NOVAK Protocol Standards Authority (NPSA)
License: NOVAK Public Safety License (NPSL)
Scope: Universal Proof-Before-Action Enforcement

---

0. FOREWORD

SP-5 defines the **mandatory requirements** for any system, organization, platform, algorithm, regulatory body, or automated process claiming compliance with the **NOVAK Execution Integrity Framework**.

The requirements herein are **normative** and enforce:

- deterministic decision-making
- cryptographic attestation
- pre-execution proof generation
- identity binding
- tamper evidence
- physical-layer resilience (PL-X)
- psycho-social adversary resilience (PS-X)
- global audit lineage (RGAC)

Compliance with this Standard is mandatory for:

- NOVAK Certification
- NOVAK Integration Approval
- Regulatory acceptance
- High-assurance deployments in government, healthcare, finance, robotics, or AI

SP-5 leverages the NOVAK Laws L0–L15, NOVAK Terminology Mappings, and the domain addenda PL-X and PS-X as foundational, non-negotiable principles.

---

1. SCOPE

SP-5 establishes requirements for:

1. **Execution Integrity Controls** (EI)
2. **Cryptographic Bindings** (HVET/EIR/RGAC)
3. **Deterministic Safety Enforcement** (Safety Gate)
4. **Identity Provenance & Attestation**
5. **Tamper-Evidence & Lineage Preservation**
6. **Physical-Layer Integrity Tolerances** (PL-X)
7. **Psycho-Social Fraud Prevention** (PS-X)
8. **Operational Governance**
9. **Certification Testing & Auditing Procedures**
10. **Continuous Compliance Monitoring**

The Standard applies to:

- digital systems

- AI/ML pipelines
- robotics
- autonomous platforms
- government regulatory workflows
- financial systems
- healthcare adjudication systems
- safety-critical automation
- public-facing decision engines

---

2. NORMATIVE REFERENCES

This Standard is built upon and depends on:

NOVAK Core Documents

- **SP-1** — Execution Integrity Standard
- **SP-2** — HVET/EIR/RGAC Cryptographic Standard
- **SP-3** — Safety Gate + PL-X + PS-X Standard
- **SP-4** — System Boundaries & Trust Surfaces
- **NTM-1** — NOVAK Threat Model
- **PBAS Category Definition**
- **NOVAK Laws L0–L15**
- **Industry Addenda PL-X & PS-X**

External References (Non-Normative)

- NIST SP 800-53 Rev.5
- ISO/IEC 27001:2022
- ISO/IEC 15408 (Common Criteria)
- NIST SP 800-90 series (Deterministic RNGs)
- FIPS-140-3
- RFC 5280 (X.509 Certificates)
- W3C Verifiable Credentials Data Model
- Dolev-Yao Adversary Model

---

3. TERMS & DEFINITIONS

(Only high-level items here; full glossary already exists in Appendix A of the whitepaper.)

3.1 Execution Integrity

The property that a system's behavior is **deterministic, auditably correct, and cryptographically validated** before any action is executed.

3.2 Proof-Before-Action (PBA)

The requirement that **proof of correctness precedes execution**, not the other way around.

3.3 HVET

Hash-Verified Execution Token. A cryptographic binding of:

- Rule (HR)
- Input (HD)
- Output (HO)

- Timestamp

3.4 EIR

Execution Identity Receipt (formerly NIPS). A signed, immutable, pre-execution evidence artifact.

3.5 RGAC

Recursive Global Audit Chain (formerly REVELATION).
A tamper-evident chronological chain of EIRs.

3.6 Safety Gate

Deterministic Safety Layer (formerly HARMONEE).
The enforcement point requiring PBA.

3.7 PL-X

Physical-Layer Integrity Addendum.

3.8 PS-X

Psycho-Social Integrity Addendum.

(Additional terms included in full glossary.)

---

4. CERTIFICATION PRINCIPLES

All certified NOVAK systems MUST:

1. **Prove correctness deterministically**
2. **Bind data, rule, output, and identity cryptographically**
3. **Block execution on mismatch**
4. **Record every approval event into EIR/RGAC**

5. **Preserve audit lineage indefinitely**
6. **Be resilient to adversaries across all threat surfaces (NTM-1)**
7. **Provide public verifiability of outcomes**
8. **Maintain transparent error modes**
9. **Operate without trusted black-box modules**
10. **Meet PL-X & PS-X integrity mandates**

📘 SP-5 — NOVAK CERTIFICATION STANDARD

PART 2 — CERTIFICATION REQUIREMENTS & CONTROL FAMILIES

---

5. CERTIFICATION REQUIREMENTS (Normative)

A system SHALL NOT claim NOVAK Certification unless it meets **ALL** requirements in this section.
These requirements are grouped into **six categories**, each derived from the NOVAK Laws (L0–L15) and the Industry Addenda (PL-X, PS-X).

5.1 Category A — Execution Integrity Requirements (EI-Controls)

These requirements govern **deterministic correctness** and **execution purity**.

EI-1 Deterministic Rule Evaluation

The system MUST guarantee that for any `Rule R` and `Input D_attested`,

```
R(D_attested) → O_deterministic
```

produces a **bit-identical output** for all runs.

EI-2 Non-Malleability of Rule Logic

Rule logic MUST be:

- pure

- side-effect-free
- versioned
- hash-verifiable

No dynamic mutation or hidden branching is allowed.

EI-3 Pre-Execution Evaluation Requirement

The system MUST NOT perform any action without:

- Evaluation
- Proof generation
- Validation
- Recording (EIR → RGAC)

EI-4 Execution Blocking Requirement

If proof verification fails:

- execution MUST halt
- the system MUST remain in a safe state
- no observable action may occur

EI-5 Public Verifiability

EIRs MUST be verifiable without proprietary systems, vendors, or secrets.

5.2 Category B — Cryptographic Binding Requirements (HVET/EIR/RGAC)

CB-1 HVET Formation Rule

A valid HVET MUST include:

```
HR = SHA-256(rule)
HD = SHA-256(data)
HO = SHA-256(expected_output)
timestamp = RFC 3339 / ISO-8601
HVET = SHA-256(HR || HD || HO || timestamp)
```

CB-2 EIR Generation Requirement

The system MUST produce an **Execution Identity Receipt** *before* any action.

CB-3 RGAC Extension Requirement

EIRs MUST be chained recursively:

```
RGAC[n] = SHA-256(RGAC[n-1] || EIR[n].HVET)
```

CB-4 Lineage Immutability

RGAC entries MUST be append-only and cryptographically irreversible.

CB-5 Identity Binding

Every EIR MUST bind identity using:

- Keypair
- Credential
- System attestation

Or an equivalent verifiable identity primitive.

5.3 Category C — Safety Gate Requirements (Pre-Execution Enforcement)

SG-1 Mandatory Enforcement

The Safety Gate MUST evaluate:

- HVET
- EIR
- PL-X (physical integrity)
- PS-X (fraud, adversary intent)

before allowing execution.

SG-2 Fail-Closed Guarantee

If evaluation fails, the system MUST default to:

```
DENY → SAFE STATE
```

SG-3 Transparent Error Mode

Errors MUST reveal:

- what failed
- why
- which boundary
- what data lineage was involved

without leaking secrets.

SG-4 Non-Bypassability

All execution pathways MUST route through the Safety Gate.
No side channel or “developer override” may exist.

5.4 Category D — PL-X (Physical Layer) Compliance Requirements

PL-1 Drift Detection

Systems MUST detect:

- clock drift
- voltage instability
- metastability
- EMI injection
- thermally induced bit errors

PL-2 Drift Modeling

Systems MUST maintain a drift model to determine:

- expected bit error tolerance
- anomaly classification
- false-positive suppression
- tamper probability weighting

PL-3 Sensor & Timing Integrity

Timing signals MUST be validated against:

- expected frequency

- jitter windows
- cross-domain timing correlation

PL-4 Hardware Tamper Evidence

Systems MUST detect:

- code morphing
- debug port activation
- firmware modification
- transient fault injection attacks

5.5 Category E — PS-X (Psycho-Social Integrity) Compliance Requirements

PS-1 Human Adversary Intent Detection

Systems MUST detect patterns indicating attempts to:

- deceive
- mislead
- bypass
- manipulate
- socially engineer
- tamper indirectly

PS-2 Cognitive Bias Mitigation

Systems MUST prevent:

- favoritism
- discrimination
- reward hacking
- adversarial framing
- ambiguity exploitation

PS-3 Fraud Pattern Recognition

Systems MUST identify:

- gradual tampering
- pattern drift
- inconsistent histories
- manipulated identities
- incongruent metadata

PS-4 Socio-Cyber Attack Defense

Systems MUST resist:

- script injection
- procedural bypass
- linguistic tampering
- feedback poisoning
- prompt engineering attacks

5.6 Category F — Organizational Controls (Modeled after ISO 27001 Annex A)

ORG-1 Governance Structure

A responsible authority MUST oversee:

- rule management
- cryptographic lifecycle
- audit review
- PL-X exception handling
- PS-X fraud escalation

ORG-2 Logging & Monitoring

Systems MUST retain:

- all EIRs
- all HVETs
- all RGAC states
- all proof failures
- all attempted bypasses

ORG-3 Change Control

Modifying:

- rules
- models
- pipelines

- hardware
- safety guardrails

requires full re-certification.

ORG-4 Training & Human Factors

Operators MUST be trained on:

- Proof-Before-Action
- PL-X/PS-X adversary classes
- lineage interpretation
- tamper evidence

---

6. NOVAK CONTROL FAMILIES (NIST-Style)

Mirrors **SP 800-53**, but adapted for Execution Integrity.

EI — Execution Integrity Controls

CB — Cryptographic Binding Controls

SG — Safety Gate Controls

PL — Physical Layer Controls

PS — Psycho-Social Controls

RG — Recursive Lineage Controls

OI — Organizational & Governance Controls

VA — Verification & Audit Controls

CM — Change Management

IM — Identity & Metadata Controls

Each family corresponds to:

- NOVAK Laws
- SP-1 / SP-2 / SP-3 / SP-4
- NTM-1 Threat Model
- PL-X / PS-X

📘 SP-5 — NOVAK CERTIFICATION STANDARD

PART 3 — ISO MAPPINGS, AUDIT CONTROLS, CONFORMANCE LEVELS, AND APPENDICES

---

7. ISO/IEC 27001:2022 ANNEX A CONTROL MAPPING (Normative)

This section provides a one-to-one mapping between NOVAK control families (EI, CB, SG, PL, PS, RG, OI, CM, IM, VA) and ISO Annex A.

This mapping is required for organizational certification audits.

7.1 ISO A.5 — Organizational Controls

ISO Control	NOVAK Control	Mapping Notes
A.5.1 Policies	OI-1 Governance	NOVAK governance defines how Execution Integrity is maintained.
A.5.7 Threat intelligence	NTM-1 Threat Model	NOVAK extends threat intel to PL-X & PS-X.

7.2 ISO A.6 — People Controls

ISO	NOVAK	Notes
A.6.3 Knowledge transfer	OI-4 Training	Operators must understand PBAS, PL-X, PS-X.
A.6.5 Disciplinary process	PS-1/PS-3	Fraud and tampering attempts require escalation.

7.3 ISO A.8 — Technological Controls

ISO	NOVAK	Notes
A.8.4 Secure code	EI-1/EI-2	NOVAK requires deterministic, pure rules.
A.8.9 Configuration mgmt	CM-1	Rule changes require re-certification.
A.8.15 Logging	RG-5	EIR/RGAC logs are mandatory.
A.8.16 Monitoring	VA-2	Continuous proof integrity monitoring.
A.8.20 Cryptography	CB-1 to CB-5	HVET/EIR/RGAC cryptographic binding.

8. TECHNICAL IMPLEMENTATION REQUIREMENTS (Normative)

This section is the **core of certification**, defining the required technical behaviors for any compliant NOVAK system.

8.1 Rule Engine Requirements

R1 — Rule Purity

- No hidden state
- No environment-dependent behavior
- No nondeterministic operations
- No time-dependent branches

R2 — Rule Versioning

Rules MUST be:

- semantically versioned

- hash-addressable
- immutable once deployed

R3 — Rule Integrity Verification

Before execution:

```
compute SHA-256(rule) => HR
compare HR to attested rule ID
```

If mismatch → execution MUST be blocked.

8.2 Data Requirements

D1 — Data Attestation

All inputs MUST be **attested**, meaning:

- checked
- validated
- identity-bound
- timestamped

D2 — Data Hashing

The system MUST compute:

```
HD = SHA-256(data)
```

D3 — Data Drift Detection (PL-X)

The system MUST detect:

- bit rot
- unexpected mutation
- value drift
- anomalous edit sequences

8.3 Output Requirements

O1 — Deterministic Output Hashing

Before execution:

```
HO = SHA-256(expected_output)
```

O2 — Predictive Integrity Window

System MUST assess whether output is **logically valid** given:

- rule
- input
- physical environment
- social context

(This validates that the output *could* be correct prior to execution.)

8.4 HVET / EIR / RGAC Requirements

H1 — HVET Formation

All systems MUST implement the exact HVET algorithm.

E1 — Mandatory EIR Generation

No operation may proceed without EIR creation.

G1 — Global Lineage Continuity

RGAC MUST maintain a continuous, irreversible chain.

G2 — Fork Avoidance

If two parallel RGAC states appear, system MUST:

- select earliest valid
- flag the other as anomaly
- block dependent operations

8.5 Safety Gate Enforcement

SG1 — Proof Evaluation Pipeline

Before execution:

1. HVET validation
2. Rule integrity validation
3. Data integrity validation
4. Output integrity validation
5. PL-X physical integrity validation
6. PS-X fraud/adversary validation
7. RGAC lineage comparison

SG2 — Fail Closed

Any failure → execution MUST stop.

8.6 Identity & Metadata Requirements

IM1 — Identity Binding

Each execution MUST include:

- system ID
- operator ID (if human)
- hardware integrity signature
- context metadata

IM2 — Revocation Handling

If identity is compromised:

- all future EIRs MUST be marked invalid
- lineage MUST remain permanent

---

9. AUDIT TESTING PROCEDURES (Normative)

Certification auditors MUST verify compliance through the following structured test plan:

9.1 Deterministic Behavior Testing

Test EI-1:
Run the same input through the rule 1,000 times:

- all outputs MUST be bit-identical
- no timing-dependent variation
- no side effects

Test EI-2:
Alter rule formatting (whitespace/noise):

- HR MUST remain consistent
- rule behavior MUST not change

9.2 Cryptographic Binding Testing

Test CB-1:
Modify input slightly → HD MUST change.

Test CB-2:
Modify rule → HR MUST change.

Test CB-3:
Modify output → HO MUST change.

Test CB-4:
Modify timestamp → HVET MUST change.

9.3 Safety Gate Testing

Test SG-1:
Introduce a PL-X anomaly (e.g., bit flip).
Execution MUST be blocked.

Test SG-2:
Introduce a PS-X anomaly (e.g., “override safety”).
Execution MUST be blocked.

Test SG-3:
Remove EIR → execution MUST be blocked.

Test SG-4:
Corrupt RGAC → execution MUST be blocked.

9.4 Lineage Integrity Testing

Test RG-1:
Tamper with RGAC:

- present state MUST detect mismatch
- system MUST default to safe state

Test RG-2:
Inject two conflicting states:

- system MUST declare “fork anomaly”

9.5 Identity Testing

Test IM-1:
Use invalid key → EIR MUST be rejected.

Test IM-2:
Try anonymized execution → MUST be blocked.

---

10. CONFORMANCE LEVELS (EI-1 → EI-5)

NOVAK certification includes five levels of assurance.

EI-1 — Basic Compliance

- Deterministic behavior
- Basic HVET/EIR
- Local Safety Gate

EI-2 — Intermediate

- PL-X drift detection
- PS-X fraud detection

EI-3 — Strong Integrity

- Full RGAC lineage
- Identity-bound EIR
- Fork detection

EI-4 — High Assurance

- Physical tamper detection
- Social adversary recognition
- Continuous verification

EI-5 — Critical Infrastructure Grade

- Multi-layer PL-X correlation
- Automated anomaly classification
- Distributed RGAC validation
- Formal verification of rule logic

- Suitable for government + medical + financial + military use

---

11. CERTIFICATION RENEWAL & REVOCATION

11.1 Renewal

- Annual review
- RGAC sampling
- Drift window recalibration
- Rule verification
- Identity re-issuance

11.2 Revocation

Certification MUST be revoked if:

- rule integrity violation occurs
- identity compromise occurs
- any attempt to bypass PBA is detected
- RGAC tampering appears
- PL-X/PS-X models are invalidated

All prior EIRs remain historically valid.

---

12. APPENDICES

Full appendices can be generated on request:

- A — Glossary
- B — Formal HVET math
- C — PL-X specification
- D — PS-X classification
- E — Standardized diagrams (SVG/PNG)
- F — Auditor Checklists
- G — API schema (JSON)
- H — Compliance questionnaire