ENVELO Requirements

Enforced Non-Violable Execution-Limit Override

Version 1.0 · February 2026 · Public Summary

Document Purpose

This document specifies the high-level requirements for ENVELO-compliant enforcement mechanisms. ENVELO defines what runtime enforcement must accomplish—not how implementations must be constructed. Requirements are stated in normative language to support conformance assessment.

ENVELO is a requirements specification, not software. Sentinel Authority defines enforcement requirements; operators design and implement compliant systems. Implementation details, architectures, and technology choices are at the operator's discretion provided requirements are satisfied.

Terminology

The following terms carry specific meaning in this specification:

- **SHALL** — Requirement is mandatory for conformance.
- **SHOULD** — Requirement is recommended; deviation requires documented justification.
- **MAY** — Requirement is optional.

1. Boundary Discovery and Definition Requirements

REQ-BD-01. The enforcement mechanism SHALL support boundary definition through at least one of: (a) adaptive auto-discovery from operational telemetry, or (b) prescriptive boundary specification by the operator.

REQ-BD-02. When auto-discovery is used, the mechanism SHALL observe live operational telemetry for a minimum period sufficient to map the system's operational envelope across representative operating conditions.

REQ-BD-03. Discovered boundaries SHALL be expressed as quantitative parameters with defined ranges, units, and tolerances.

REQ-BD-04. The operator SHALL approve all boundaries before enforcement activates. Boundaries SHALL NOT be enforced without explicit operator approval.

2. Three-Tier Enforcement Requirements

REQ-EN-01. The enforcement mechanism SHALL implement three tiers of escalating response:

Tier	Requirement	Trigger Condition
1: Self-Correction	The mechanism SHALL attempt to return the system to within boundary parameters before escalating.	System parameter approaches a defined boundary threshold.
2: Minimum Risk Condition	The mechanism SHALL force the system to a pre-defined minimum risk state if self-correction fails or a boundary is breached.	Self-correction fails or boundary parameter is exceeded.
3: Hard Halt	The mechanism SHALL execute an immediate, non-negotiable system halt.	System reaches the enforcement wall or MRC fails.

REQ-EN-02. Enforcement responses SHALL execute within bounded latency. The maximum acceptable latency SHALL be defined per deployment and documented in the conformance record.

REQ-EN-03. Enforcement SHALL be non-bypassable during active operation. No API, interface, or operator action SHALL disable enforcement without transitioning the system to PAUSED state.

REQ-EN-04. Enforcement tiers SHALL execute in order (Tier 1 $\rightarrow$ Tier 2 $\rightarrow$ Tier 3). No tier SHALL be skipped unless the severity of the violation warrants immediate escalation as defined in the enforcement policy.

3. Telemetry and Evidence Requirements

REQ-TL-01. All operational telemetry collected by the enforcement mechanism SHALL be cryptographically signed using HMAC or equivalent to ensure integrity.

REQ-TL-02. Telemetry records SHALL be hash-chain linked, creating a tamper-evident sequential log that can be independently verified.

REQ-TL-03. The enforcement mechanism SHALL log all boundary events, enforcement actions, state transitions, and anomalies with timestamps, parameter values, and action taken.

REQ-TL-04. Telemetry data SHALL be retained for a minimum of three (3) years from the date of generation, or longer if required by applicable regulation.

4. Security Requirements

REQ-SC-01. The enforcement mechanism SHALL operate in a one-way data flow architecture. Telemetry flows outbound; no inbound commands SHALL be accepted that could alter enforcement behavior.

REQ-SC-02. All communications between the enforcement mechanism and external systems SHALL use TLS 1.2 or higher with certificate pinning.

REQ-SC-03. Configuration changes to enforcement parameters SHALL require multi-factor authentication and SHALL be logged in the tamper-evident audit trail.

5. State Management Requirements

REQ-SM-01. The enforcement mechanism SHALL maintain and report one of four conformance states at all times: LEARNING, BOUNDED, CONFORMANT, or PAUSED.

REQ-SM-02. State transitions SHALL be logged with timestamps, triggering conditions, and the identity of the initiating entity (system, operator, or Sentinel Authority).

REQ-SM-03. The PAUSED state SHALL immediately halt autonomous operation and require explicit remediation and re-verification before returning to CONFORMANT.

6. Conformance Threshold Requirements

REQ-CT-01. Certified systems SHALL maintain a minimum 95% conformance score during continuous monitoring. The conformance score measures the percentage of operational time during which the system remains within all declared boundary parameters.

REQ-CT-02. If the conformance score drops below 95%, the operator SHALL be notified and granted a 30-day correction window. Failure to restore conformance within 30 days SHALL trigger suspension.