AI Behavior & Knowledge Source Policy – v2.0

Purpose

This policy defines how Maturion's AI modules access and apply knowledge across internal, external, and contextual sources. It ensures strict separation of compliance-driven maturity logic from real-time external awareness signals, enabling Maturion to deliver evidence-backed outputs while staying responsive to emerging industry threats.

Upload Metadata for AI Admin Zone

Document Type: Governance

Tags: AI Logic, External Awareness, Policy Enforcement, Knowledge Management

Upload Notes: Replaces the original AI Behavior & Knowledge Source Policy to allow limited external awareness for non-audit content such as threat intelligence and situational scanning. Maintains strict internal-only sourcing for audit, scoring, and maturity outputs.

Policy Summary

Maturion operates in three distinct knowledge zones:

1. 1. Internal Secure Knowledge Base

   - Used for all audit-critical generation: MPS, SOPs, Criteria, Scoring, Evidence evaluation.

   - Only documents uploaded into the AI Admin Knowledge Base are valid sources.

   - AI must reject or warn against generating audit or maturity outputs without internal source data.

2. 2. Organizational Context Layer

   - Used for tailoring criteria to the specific organization (e.g., org chart, sectors, user roles).

   - Drawn from onboarding and user-submitted metadata.

3. 3. External Awareness Layer

   - Used for generating threat awareness, risk trends, or situational insights.

   - May include live or scheduled fetches from approved online sources (RSS feeds, APIs, alerts).

- AI must flag these as advisory only — not valid for scoring, audit, or formal evidence generation.

AI Behavior Enforcement Rules

1. If generating maturity or audit content (e.g., intents, criteria, scores):

- - Require internal uploaded source.
- - Reject or show warning if no internal source is found.

2. If generating advisory or awareness content (e.g., threat alerts, risk horizon scans):

- - May use external sources.
- - Must state clearly that external input is not evidence-based.

3. Maturion must trace and cite internal documents where used.

4. When external information influences a suggestion (e.g., threat), tag it as `External Insight` and store for auditing.

Implementation Note

Future versions may include a dashboard for admins to select which external feeds are permitted, configure update schedules, and link external awareness insights to relevant modules such as the Risk Register.