

GRIDBASE COMPLIANCE TEMPLATE

DOC ID: GB-GOV-2026-07

SUBJECT: TEMPORAL SYSTEM SNAPSHOT (V1)

PHASE: AUDIT & LOGGING

[SECTION 1: TEMPORAL METADATA]

- [] Timestamp (UTC): YYYY-MM-DD HH:MM:SS
- [] Target System/Endpoint: [Specify API or VPC instance]
- [] Base Model Weights: [e.g., Llama-3-70B-Instruct / Mistral-Large]
- [] Active System Prompt Hash (SHA-256): [Insert Hash]

[SECTION 2: ADVERSARIAL RESILIENCE LOG]

- [] Assess current baseline against MITRE ATLAS™ AML.T0096 (API Exploitation).
- [] Record Perplexity Thresholds for semantic anomaly detection.
- [] Validate Human-in-the-Loop (HITL) override functionality for agentic workflows.

[SECTION 3: JURISDICTIONAL ALIGNMENT]

- [] Document UI transparency disclosures (EU AI Act alignment).
- [] Verify isolation of Tier-1 Proprietary Data from the retrieval-augmented generation (RAG) vector space.
- [] Confirm data sanitization protocols are active for all newly ingested vectors.

[SECTION 4: DOCTRINE OF TEMPORAL SECURITY]

- [] Acknowledge that this Snapshot represents the system's defensive posture solely at the recorded timestamp.
- [] Mandate a new Snapshot assessment upon any modification to model weights, system prompts, or tool access permissions.

ADVISORY: SECURITY IS A TEMPORAL STATE. THIS DOCUMENT DOES NOT MITIGATE FUTURE LATENT VULNERABILITIES OR RECURSIVE INJECTIONS.