5.1 Audit & Event Ledger — Canonical Specification

Version: v1.0

Status: Canonical / Build-Blocking

Owner: Pearl & Pig (Jon Hartman)

Applies To: GARVIS / Telauthorium / MOSE / TELA / Pig Pen / UOL / ECOS

Effective: Immediate

Purpose

This document defines the immutable audit and event ledger for the GARVIS Full Stack.

The ledger is the authoritative record of what happened, when it happened, under whose authority, and why.

If it is not in the ledger, it did not happen.

Core Principles (Non-Negotiable)

- Append-only (no deletes, no edits)
- Immutable once written
- Time-ordered
- Authority-linked
- System-agnostic

The ledger records events, not interpretations.

Event Types (Canonical)

Every ledger entry must be one of the following event types:

1. Authorship Event — creation or attribution of a TID
2. Decision Event — a human decision resolution
3. Routing Event — MOSE operator selection or sequencing
4. Enforcement Event — block, halt, or constraint trigger
5. Execution Event — TELA action attempt or completion
6. Rights Event — rights assignment, change, or restriction
7. Overlay Event — UOL attachment or detachment
8. Registry Event — operator status change (suspend/revoke)
9. Version Event — system or document version change

Required Event Fields

Every event must include:

- event_id
- event_type
- timestamp
- tid
- authority_taid
- source_system (Telauthorium / GARVIS / MOSE / TELA / Pig Pen / UOL)
- event_summary
- event_payload (structured, non-freeform)
- previous_event_hash (for chain integrity)

Authority Resolution Rules

- Every event must resolve to a human TAID
- System-generated events must include the responsible TAID
- TAI-D identifiers may appear as actors, never as authority

No anonymous events are permitted.

Chain Integrity

- Events are cryptographically chained via previous_event_hash
- Breaking the chain invalidates downstream trust
- Hash verification is mandatory on read

Write Rules

- Only authorized system components may write events
- Events are written after successful state change
- Failed attempts still generate enforcement or execution-failure events

Read Rules

- Ledger is readable by GARVIS at all times
- Human visibility is permission-gated
- Pig Pen operators may never read raw ledger entries

Audit & Dispute Posture

The ledger is:

- The source of truth for audits
- Admissible for dispute resolution
- Non-repudiable

Historical events may not be re-interpreted or re-written.

ECOS & Tenant Boundaries

- Each tenant maintains a logically isolated ledger view

- Cross-tenant reads are prohibited
- Pearl & Pig retains root verification authority

Canon Lock

This document defines the Audit & Event Ledger v1.0.

Any change requires a new version, founder authorization, and a published delta log.