

2.2 GARVIS ↔ Telauthorium — Enforcement, Contract & Engineering Specification

Version: v1.0

Status: Canonical / Implementation-Ready

Applies To: All GARVIS, ECOS, and Telauthorium deployments

PART I — GARVIS ↔ Telauthorium Enforcement Map

1. Authority Relationship

- Telauthorium is the sovereign authority for authorship, provenance, and rights
- GARVIS is the sovereign intelligence for reasoning, routing, and execution
- GARVIS cannot override Telauthorium
- Telauthorium can block GARVIS

Telauthorium answers “Is this legitimate?”

GARVIS answers “What should happen next?”

2. Enforcement Matrix (Who Blocks What, When)

Event	Telauthorium Check	Result
Object created	TID required	Block if missing
Authority assigned	TAID validation	Block if unresolved
AI-generated output	Human TAID resolution	Block if absent
Modification attempt	TAID scope check	Block if unauthorized
Licensing action	Rights state validation	Block if unclear
Deployment request	Rights + authority check	Block if invalid

Event	Telauthorium Check	Result
Provenance break	Lineage continuity	Block and flag
System execution	TID/TAID presence	Halt execution

Rule: If Telauthorium returns invalid, GARVIS must halt, log, and surface the failure.

3. Failure Handling

When blocked by Telauthorium, GARVIS must:

1. Halt execution immediately
2. Preserve state (no rollback mutation)
3. Log failure with TID reference
4. Surface remediation requirement

No automatic override is permitted.

PART II — Contract-Ready Appendix (Zero Fluff)

1. Definitions

Telauthorium: The authoritative system of record for authorship, provenance, and rights.

TID: Telauthorium ID — immutable identifier for a registered object.

TAID: Telauthorium Authority ID — scoped authority over a TID.

GARVIS: Sovereign intelligence layer that operates subject to Telauthorium constraints.

2. Ownership

- Pearl & Pig retains ownership of Telauthorium and GARVIS systems
 - Clients may own content registered within Telauthorium
 - System ownership is never transferred
-

3. Authority & Liability

- All content must resolve to a human TAID
 - System authorities act under delegated mandate only
 - Liability resolves to the highest-scope human TAID
-

4. Rights Enforcement

- Rights states are enforced automatically
 - Execution, licensing, or deployment halts on ambiguity
 - No implied rights are granted
-

5. Audit & Dispute

- Telauthorium records are authoritative
 - Provenance logs are admissible for audit and dispute resolution
 - Historical records are immutable
-

PART III — Engineering Handoff Specification

1. ID Lifecycle

Creation

- Generate TID at object inception
- Assign primary human TAID

Mutation

- Version increments retain original TID
- Authority scope revalidated

Delegation

- Assign TAID-D with scope + expiry

Revocation

- Revoke TAID without altering provenance
- Record revocation event

Archival

- Lock TID as read-only
-

2. Revocation Rules

- TAIDs may be revoked by Pearl & Pig or originating human authority
 - Revocation does not delete history
 - Revoked TAIDs lose execution, licensing, and modification rights
-

3. Required System Checks (Pseudologic)

```
if not TID:
    block()

if not resolve_human_TAID():
    block()

if action in [modify, license, deploy]:
    validate_TAID_scope()

if rights_state unclear:
    halt_execution()
```

Canon Lock

This document defines the binding enforcement, contractual, and engineering rules governing GARVIS ↔ Telauthorium interaction.

Any change requires a new version and explicit founder authorization.