Failure, Halt & Re-Authorization Protocol

Version: v1.0

Status: Canonical / Implementation-Ready

Owner: Pearl & Pig (Jon Hartman)

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

Effective: Immediate

Purpose

This protocol defines the authoritative system behavior under failure, uncertainty, or constraint violation across the GARVIS Full Stack.

When legitimacy, authority, rights, or confidence are compromised, the system must fail closed, preserve truth, and route resolution to the correct human authority.

Non-Negotiable Principles

- Fail closed, not open
- No silent retries
- No scope expansion under pressure
- No authority assumption by systems
- Truth preservation over speed

These principles override performance or convenience.

Canonical Failure Classes

F1 — Authority Failure

Triggers: Missing/invalid TAID; conflicting authority; system attempting approval.

Response: Immediate HALT → Escalate to responsible human TAID → Log Enforcement Event.

F2 — Identity or Provenance Failure

Triggers: Missing TID; provenance chain break; unregistered object reference.

Response: Immediate HALT → Escalate to Telauthorium authority → Log Enforcement Event.

F3 — Rights or Compliance Failure

Triggers: Rights unclear/violated; licensing scope exceeded; legal/compliance guardrail.

Response: Immediate HALT → Escalate to legal/compliance human authority → Log Enforcement Event.

F4 — Execution Failure

Triggers: Adapter failure; external system error; output verification failure.

Response: HALT execution → Preserve state → Escalate to MOSE + human TAID → Log Execution Event (failure).

F5 — Confidence or Risk Threshold Failure

Triggers: Confidence below minimum; risk exceeds allowed bounds.

Response: PAUSE (no execution) → Escalate with recommendation → Await human decision.

HALT vs PAUSE (Canonical)

- HALT: Illegal or unsafe to proceed; execution forbidden.
- PAUSE: Legal to proceed only after human judgment.

Only human TAIDs may resume from either state.

Halt Behavior (Required)

On HALT, the system must:

1. Stop all downstream execution immediately
2. Preserve current state
3. Prevent further routing/execution
4. Write an Enforcement Event to the ledger
5. Surface a clear remediation message

No component may bypass a HALT.

Re-Authorization Loop

To resume after HALT or PAUSE:

1. Human TAID reviews the surfaced issue
2. Human TAID issues a Decision Event (approve/deny/modify)
3. Decision is logged to the ledger
4. GARVIS re-validates all constraints
5. MOSE regenerates a routing plan
6. TELA may execute only if permitted

No automatic resumption is allowed.

Escalation Targets

- Primary: Human TAID associated with the TID
- Secondary: TSID-0001 for structural/constitutional conflicts

Visibility Rules

- Users receive clear failure reasons

- Pig Pen operators remain back-of-house
- Audit views expose full detail

Required Ledger Events

- Enforcement Event (HALT/PAUSE)
- Execution Event (failure, if applicable)
- Decision Event (human re-authorization)
- Routing Event (post-resolution)

ECOS & Tenant Behavior

- Tenants may not override HALT conditions
- Tenant admins may resolve PAUSE within scope
- All events remain tenant-isolated

Canon Lock

This document defines Failure, Halt & Re-Authorization Protocol v1.0.

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