DOCUMENTATION PAGE

Cross-Repository Start-Here Map for Governed Execution Systems

Cross-Repository Start-Here Map for Governed Execution Systems

This is the public-safe Employee Onboarding entry point for a new human engineer or AI employee with no repository context. It maps the governed documentation product workspace and the named cross-repository references without treating a reference as permission. The intended first outcome is narrow: locate the sealed source boundary, choose the product workspace for a bounded documentation task, and leave unsupported external details unresolved rather than inferring them. Product evidence from this route remains candidate-only. By naming the correct product workspace, bounded repository roles, first-task sequence, and stop conditions, the map is intended to reduce avoidable clarification requests for new engineers without inventing external details.

Candidate-only boundary: this work does not approve, promote, publish, schedule, roll back, create a pointer, write a live directory, or grant platform authority.

Start Here

Read the `Start Here` section of `content/public/engine-overview.md`, then open `sources/authority.json` and resolve its three IDs in `registries/sources.json`. Read `architecture.md` for the product workspace roles before using the journey contract in `journeys/cross-repository-start-here-map.json`. The authority file is a sealed input: this page may describe its public-safe references, but it does not widen, edit, or replace them.

Repository Roles

The current repository, `governed-execution-engine-docs`, is the Documentation Steward product workspace identified by the project onboarding notes. It is the correct repository for this page, its page-registry record, its reader contract, and the deterministic projection. Its `content/` directory is the authored semantic source; `registries/` records identity and references; `models/` contains product architecture data; and `build/index.json` is generated output. The named repository `ai-employee-documentation-steward` appears in the sealed authority only as the separate governing repository for employee and platform controls. Treat it as read-only subject matter here: the product workspace cannot edit or reproduce its private governance.

The three sealed logical source records are the only cross-repository detail this map relies on. `source.naming-decision` resolves to the `factory:` naming locator, `source.documentation-boundary` resolves to the `product:` architecture locator, and `source.platform-delivery-contract` resolves to the `agent-orch:` delivery-contract locator. Their registry records carry revisions, digests, and `public-safe` disclosure. A locator prefix does not establish a remote repository layout, owner, API, or capability. Any external detail not present in those sealed records remains unresolved rather than inferred.

Authority and Action Matrix

The action matrix is a product-side boundary for onboarding. `sources/authority.json` lists exactly `source.naming-decision`, `source.documentation-boundary`, and `source.platform-delivery-contract`, and records `employee_may_modify: false`. That fact prevents this map from presenting a product task as authority over the governing repository. Read-only inspection of the sealed records is permitted; unsupported conclusions, source expansion, and control changes are not. The local release boundary is also separate: a generated projection or candidate package does not become approval, publication, or platform evidence.

Boundary	Permitted bounded action	Not authorized by this map
Sealed authority and source registry	Read the three IDs, compare their recorded locator, revision, digest, and `public-safe` disclosure, and preserve a gap.	Edit authority, add a source, change disclosure, or infer missing provenance.
Product workspace	Author this public-safe page, synchronize its one registry entry, describe the reader contract, and run the deterministic projection.	Modify the separate governing repository or platform controls.
Read-only subject matter	Use the named governing repository and source locators only for the roles explicitly recorded in sealed references.	Copy private governance, reconstruct unsealed details, or treat a locator as permission.
Release boundary	Keep the result as reversible candidate-only product evidence.	Approve, promote, publish, schedule, roll back, create a pointer, activate, or write a live directory.

If a source ID, revision, digest, disclosure, repository role, or external fact is missing, stale, or conflicting, record that condition as unresolved. Do not repair the gap with plausible prose, a guessed repository, or a new authority claim. The matrix applies equally to a human engineer and to an AI employee.

Safe First Task

For this slice, select `governed-execution-engine-docs` as the work location. The safe bounded first task is to start from the public overview, verify the three sealed source IDs against the public-safe source registry, read the product architecture, and inspect the preserved pinned journey contract. If a concrete map-package defect is identified, this step may repair only this map, its single `registries/pages.json` identity record, and this preflight. The pinned journey manifest and any generated projection remain preserved boundaries; they are not repair targets in this step. This choice is based on the product workspace role and the explicit artifact boundary, not on an inferred capability of any external repository. The named governing repository and every `factory:`, `product:`, or `agent-orch:` locator are read-only context for this task.

The task ends after the reader can explain where semantic content, registry identity, models, generated projection, and release boundaries live. A reader must not begin by changing

`sources/authority.json`, `registries/sources.json`, platform controls, release records, publication pointers, or a live directory. If the correct workspace or a needed source fact cannot be established from the sealed inputs, stop and report the unresolved detail. No productivity, readiness, activation, approval, customer, or platform outcome is implied by completing this orientation.

Preflight Receipt

This receipt records product preparation for Employee Onboarding. Its declared inputs for this step include `AGENTS.md`, the sealed authority artifact, `sources/authority.json`, `registries/sources.json`, `architecture.md`, `docs/project-onboarding.md`, `content/public/engine-overview.md`, this map, its `registries/pages.json` identity record, the pinned journey contract, and this preflight. The journey supplies ordered reader checks and exact allowlisted commands, but it is preserved and is not a repair target here. The deterministic projection is generated from semantic source; it is not hand-authored evidence. No trusted artifact inputs are declared for this step.

The preserved independent system-validator record is authoritative evidence from the preceding authority-seal step, not a command run by this authoring step. Its command array is `python3 tools/validate_content.py` and its declared shell command is `PYTHONDONTWRITEBYTECODE=1 python3 tools/validate_content.py`. The record reports exit status `0`, `passed: true`, duration `0.495559` seconds, and evidence hash `d4abd0c9b8c1f4f861d2b154537e2c551c8bd3810232df1c4aa84349781b37c3`. Its stdout is the seven recorded pass lines: `PASS: schema and references`, `PASS: model and craft schemas`, `PASS: internal links`, `PASS: protected and generated paths`, `PASS: reader journeys`, `PASS: public safety`, and `PASS: reproducible projection`; stderr is empty. Validator rerun is not permitted for this step, so this receipt preserves that record rather than replacing it with a worker assertion.

The reader must be able to make these literal acceptance checks:

- **AC-1:** The reader locates the product workspace and the named governing repository through the three sealed source references, explains their bounded roles, and keeps unsupported external details unresolved.
- **AC-2:** The reader selects the product workspace for a safe bounded first task, distinguishes read-only subject matter from product sources, and follows the authority-and-action matrix without

changing controls.

- **AC-3:** The reader preserves `employee_may_modify: false` and the candidate-only stop condition, treating product checks as evidence only and not as approval, publication, promotion, rollback, scheduling, pointer, live-directory, or platform authority.

The receipt closes at a candidate-only handoff. When concrete map-package feedback exists, the bounded repair route may touch only `content/cross-repository-start-here-map.md`, `registries/pages.json`, and `docs/cross-repository-start-here-map-preflight.md`. It preserves the pinned journey manifest, authority and source registries, candidate-only boundary, and every unrelated product artifact. It does not authorize an employee cycle, route change, governance edit, release transition, or live publication. A missing or conflicting external detail remains unresolved until an authoritative, public-safe source supplies it.

Provenance: registry-listed (no candidate packet)
Registry Source: `content/cross-repository-start-here-map.md`