Veriscopic Governance Evidence System — Locked Architecture & Operating Model

Status: Locked / Production-ready (v1.2) 280126

This document is the authoritative reference for how Veriscopic's governance, evidence packs, and drift detection system functions.

Its purpose is to:

- Prevent accidental duplication or regression
- Onboard future developers or AI agents safely
- Clearly separate *what is locked* vs *what may evolve*

If behaviour appears inconsistent, this document is the source of truth.

---

1. Core Design Principle (Non-Negotiable)

Veriscopic does **not** monitor organisations in real time.

It records **declared governance facts**, seals them into immutable Evidence Packs, and compares those sealed snapshots over time.

Everything flows from this.

> Evidence is fixed in time. Drift is comparative, not live.

---

2. Canonical Objects

2.1 Evidence Pack (Authoritative Snapshot)

An Evidence Pack is the **only canonical governance snapshot**.

It includes:

- Accepted legal documents (with version + content hash)
- AI systems registry (declared state)
- Responsibility map (organisation-level accountability declarations)
- Integrity metadata (canonical JSON hash, algorithm, generation time)

Evidence Packs are:

- Append-only
- Cryptographically verifiable
- Never mutated after creation

Source of truth:

- `/lib/legal/export-evidence.ts`
- Persisted in `evidence_packs` table

2.2 Feature Gating — `evidence_pack`

The ability to export Evidence Packs (PDF / JSON) is gated by:

- `organisations.features.evidence_pack = true`

This gate is enforced:

- In the API layer (`requireFeature`)
- Not via UI alone

If disabled:

- `/api/evidence-pack/pdf`
- `/api/evidence-pack/json`

must return 403

---

3. Drift Detection (v1 — Locked Semantics)

3.1 When Drift Runs

Drift detection runs **only when a new Evidence Pack is generated**.

Specifically:

- JSON export triggers drift
- PDF export does *not* trigger drift

This is intentional and defensible.

3.2 Drift Scope (Explicit)

Drift compares:

> The two most recently sealed Evidence Packs.

Governance changes made *after* the latest pack:

- Do **not** appear immediately
- Are reflected only when the **next** Evidence Pack is generated

This scope is now explicitly stated in:

- Dashboard UI
- Drift report page
- Drift appendix PDF

3.3 Drift Severity Model

Defined in:

- `/lib/legal/drift/materiality.ts`

Rules (v1):

- **Material drift** → previously asserted assurance may no longer hold
- **Informational drift** → change detected, assurance not weakened

Examples:

- Legal acceptance changes → always material
- AI system risk-relevant field changes → material
- Additions → informational

---

4. Drift Outputs

4.1 Drift Events

Each drift run creates a `drift_events` row containing:

- `from_pack_hash`
- `to_pack_hash`
- Drift summary
- Full itemised delta

This table is append-only.

4.2 Drift Appendix PDF

File:

- `/lib/legal/export-drift-appendix-pdf.ts`

Key guarantees:

- Explicit drift scope
- Prominent pack hashes
- No implication of live monitoring

The PDF is *explanatory*, not authoritative. The JSON + hashes are authoritative.

---

5. Responsibility Map Semantics

Responsibility records:

- Are organisation-level declarations
- Do **not** assign personal liability
- Do **not** certify compliance
- Do **not** monitor behaviour

They exist to:

- Define accountability surfaces
- Define expected evidence
- Be sealed into Evidence Packs

UI distinction is intentional:

- Organisation may be "accountability declared"
- While having zero individual responsibility rows

This is not a contradiction.

---

6. Audit Logging

Audit events are:

- Best-effort
- Non-blocking
- Append-only

RLS failures on audit inserts:

- Must never block core actions
- Are acceptable by design

---

7. Supabase Contract (Do Not Break)

Key invariants:

- Evidence packs are immutable once written
- Drift compares packs, not live tables
- Feature flags are enforced server-side
- RLS must allow reads for verification, not mutation

Tables that must remain append-only:

- `evidence_packs`
- `drift_events`
- `organisation_audit_events`

---

8. What Is Safe to Extend (v2+)

Allowed:

- UX banners ("governance inputs changed — re-export to assess drift")
- Auto-trigger drift on additional events (optional)
- Additional evidence sections

Not allowed without redesign:

- Live drift
- Implicit monitoring
- Mutating past evidence

---

9. If Something Seems Wrong

Ask, in order:

1. Was a new Evidence Pack generated?
2. Which pack hashes are being compared?
3. Is the feature flag enabled?

If those answers align, the system is behaving correctly.

This document is authoritative. If future code or prompts conflict with it, this document wins.