AUDIT-TRAIL-SPEC

Layer 2 Procedural File 2 of 6 — The Dash / NornGate at SBS Implements: 00-Take-Notice.md (status), 00-NornGate-Architecture.md (gate transits). Operated by: Urd (custody), within Mimir's retention classes.

Purpose

Schema and integrity for the sealed ledger beneath The Dash. Every gate transit, authorization, execution, reconciliation, and incident is a record. The ledger's job: make the fleet's posture provable — to the board, to auditors, to counsel, to the FCC, to a court.

Storage Architecture — Three Layers

- **Hot:** PostgreSQL on the DigitalOcean production server — current operational records, fast retrieval.
- **Warm:** object storage — aged records, standard retrieval.
- **Cold (WORM):** object-lock compliance mode — non-rewritable, non-erasable for the retention term. Financial and gate-transit records age here on schedule.

Per-Record Schema

record_id · timestamp · agent · action_type · Governance-Gate category · gate transits (G0–G4 with verdicts) · authorization handle (G2) · inputs_hash · outputs_hash · status-preamble reference · foreign keys (sequence linkage) · retention class.

The Four-Record Sequence

Every material action closes a sequence: **plan (Odin) → authorization (G2 handle) → execution (Thor) → verification (Sif / Urd)**. Completeness checking is sequence closure: an execution record without its authorization handle is an anomaly; an authorization without execution is an open obligation. This is the ledger's completeness proof.

Hash-Chain Mechanics

Each record embeds the SHA-256 of its canonical serialization plus the hash of the prior record. Tampering anywhere in the chain is detectable in O(n) by recompute. Canonical documents (Layer 1/2 files) are sealed by the same construction — see any file's Document Control footer.

Retention Schedule (binds Mimir's classes)

- Financial records: seven-year immutable (SOX § 802-grade WORM).
- Gate transits: permanent.
- Ephemeral working memory: expires by policy.
- Litigation/dispute hold: extends any class indefinitely; the hold itself is a policy_change-class record; tier-aging suspends automatically for held records. Holds are instituted through G2 (BR-class).

Access Control & Audit-of-Audit

Subject roles: fleet agents (own scope only) · IT Director (full read) · auditor role (full-trail visibility, read-only) · break-glass (logged, reviewed). **Every access is itself a record** — who accessed what, when, under which handle — defending against any later allegation of selective access.

Integrity-Verification Cadence

- **Continuous:** daily chain verify · weekly cross-seal · monthly full recompute · quarterly restore drill · annual input to the oversight package.

- **On-demand:** incident response (any SEV), auditor request, customer dispute, regulatory or counsel inquiry. On-demand verification produces the defense substrate within hours, not weeks.

The Fleet Oversight Package (quarterly)

The documentary basis the human board reviews the fleet against: 1. Audit-trail integrity report for the quarter; 2. Cross-agent reconciliation completeness summary (Sif); 3. SEV-1 / SEV-2 incident inventory (Hel's classifications); 4. Continuous-verification cadence report; 5. Break-glass usage log and roster status (Single-Maintainer-Appendix); 6. Policy-change register (policy_change-class records). Assembled by Frigg, drafted by Bragi, issued in the SBS report design system, approved through G2 before release.

Authoritative For

Outside-auditor control-environment review; counsel's diligence on the fleet's posture; dispute evidence; oversight-package production.

What's Not Here

Authorization categories (10-Governance-Gate-Spec); incident runbooks (00-Incident-Response-Matrix); defense-surface mapping (10-Defense-Posture).

Modification Protocol

Proposal drafted by the responsible agent → legal/sufficiency review where statutory interpretation is implicated → Odin staffs the synthesis pass → G2 request with full evidence package → human decision per the Single-Maintainer-Appendix authority structure. Approved modifications are versioned (1.0 → 1.1 minor; 1.x → 2.0 material) and captured in Urd's ledger as policy_change-class records. Layer 1 files are not modified by this protocol — they require SBS Board / IT Governance authorization via Asgard Policy Review.

Document Control: SBS-DASH-PROC-02 · v1.1 · 2026-08-05 · SHA-256 (content above): 54ef…e249 · Sealed under Audit-Trail-Spec § 8.2. Modification authority: SBS Board / IT Governance via Asgard Policy Review (Governance-Gate); revalidation propagates per Tyr-SKILL § 3.4.

Revision #1
Created 2026-08-05 04:11:36 UTC by SBS Admin
Updated 2026-08-05 04:12:17 UTC by SBS Admin