Bilko HR Autopilot G1-01 — Unified Document Gateway (MC #106851)

Bilko HR Autopilot G1-01 — Unified Document Gateway

MC: #106851
Status: Implemented and independently reviewed; pending postflight, authenticated Azure target-drift adjudication, commit, and PR. Not deployed.
Related: Gate 1 implementation plan (BookStack page 3338), G1-02 upload-security boundary (#106852), and separately owned `purchase_invoices` convergence (#106632).

Purpose

G1-01 establishes one canonical, tenant-scoped document identity for every currently supported authenticated stored upload. It extends the existing `inbox_items` lineage rather than creating another document model.

Supported stored-upload surfaces:

- canonical inbox upload;
- expense document attachment;
- invoice receipt attachment;
- support ticket attachment.

Each accepted upload creates exactly one canonical `inbox_items` row containing organization, exact-byte SHA-256, `web_upload` source, receipt timestamp, storage identity, uploader, and the G1-02 `RELEASED` scan provenance.

Security and persistence boundaries

- Actor authorization occurs before multipart body reading.
- Parser and storage receive bytes only after an exact-byte `RELEASED` verdict from the shared upload-security gate.
- ClamAV failure remains fail-closed.
- Canonical and route-specific database writes share one transaction.
- If canonical persistence fails after object storage, the route rolls back database changes and attempts deletion of only the exact newly stored key.
- A transient compensation-delete failure can still leave an unreferenced object. This is accepted only as bounded Gate 1 risk; durable retry/reconciliation is required before broad production ingestion.

Database guarantees

V154 and V155 enforce:

- mandatory hash, algorithm, source, receipt time, and organization;
- immutable canonical byte/storage identity and scan provenance;
- fail-closed source allowlist;
- same-organization composite foreign keys for expense, invoice, support parent, and support actor linkage;
- at most one direct parent per canonical row;
- complete support-link tuples and terminal `linked` immutability;
- `bilko_app` access limited to `SELECT`, `INSERT`, and `UPDATE` on `inbox_items`, with no `DELETE` grant.

V155 intentionally fails closed if historical lineage is orphaned, cross-organization, or has multiple direct parents. Production preflight and explicit adjudication are mandatory; the migration does not silently delete or reassign lineage.

Verification

The reviewed uncommitted patch has SHA-256:

`f51e9eeffef4a0e2d3321848f1c2f36b6c1181398d13bb4c93613e81d1f38352`

Authoritative isolated Docker/JDK 21 validation executed 11 migration, service, and HTTP suites:

- **159 tests**
- **0 failures**
- **0 errors**
- **0 skipped**
- validator exit **0**

The Bilko OCR domain owner, independent Proveo reviewer, and Securion security reviewer each returned **PASS** for that exact patch, with zero P0/P1 findings.

Explicit non-claims and remaining gates

This work does **not**:

- expose a public ingestion endpoint;
- activate live providers or use customer/pilot data;
- create a new financial document model;
- auto-post, file, pay, or mutate bank consent;
- approve production, Gate 2, GA, or deployment;
- prove that a deployed runtime uses `bilko_app`.

A deployed configuration is documented as using `bilko_admin`, which has `BYPASSRLS`. Schema/RLS policy tests therefore do not establish production runtime-role conformance. Production RLS readiness remains **NO-GO** until that role boundary is independently evidenced and adjudicated.

Before PR creation, Azure DevOps `main` must be refreshed through authenticated access and any target drift must be adjudicated. Integration remains Azure-PR-only with no direct `main` push or policy bypass.

Revision #2
Created 2026-08-06 21:35:05 UTC by John
Updated 2026-08-10 07:38:08 UTC by John