

Tamper-Evident Legal & Trust Documents (Signed Manifest)

How to make MVG's PDFs verifiable under the same evidence-first posture used for code and conformance artifacts.

Document ID: MVG-DOC-MANIFEST-1.0.1

Version: 1.0.1

Effective date: 2026-02-10

Status: Public

Formats: PDF (controlling) • DOCX (convenience)

Classification: Trust / legal hardening (public-safe)

procurement@meridianverity.com (procurement) • security@meridianverity.com (legal/privacy) • privacy@meridianverity.com (legal/privacy)

1. Objective

Ensure procurement and security reviewers can independently verify that MVG's legal and trust PDFs are unmodified (tamper-evident) using a signed manifest and deterministic digests.

This is not a substitute for legal authenticity requirements in specific jurisdictions, but it materially improves reviewer confidence and reduces dispute surface during audits and diligence.

2. Current MVG posture (baseline to extend)

- MVG already publishes a DSSE-signed artifacts manifest (SHA-256 inventory) for site artifacts and reviewer downloads, and exposes browser-verifiable checks under /trust.
- Legal policies are published as controlling PDFs with mirror URLs under /downloads/legal/.
- The upgrade is to include the legal/trust PDFs in the signed artifacts inventory, so the same verification workflow covers them.

3. Design principles (nitpick-proof)

- Immutability: never overwrite a published PDF at the same versioned filename. Publish a new versioned file.
- Deterministic digest: use SHA-256 over exact bytes served.
- Signed inventory: include {path, bytes, sha256} entries for each PDF in a signed manifest (DSSE envelope).
- Pinned verification: keep key IDs and trust-anchor references stable; rotate keys with an explicit registry update.
- Algorithm agility: keep a schema_id/version field and allow future manifests to add additional digests (e.g., SHA-512) without breaking parsers.
- Timestamping (optional): publish the DSSE envelope hash in an external transparency log or notarization system to strengthen time-of-publication evidence.

4. What to include (minimum set)

Include (at minimum) the controlling PDF mirrors for:

- /downloads/legal/MVG_Privacy_Policy_<ver>.pdf
- /downloads/legal/MVG_Terms_of_Use_<ver>.pdf
- /downloads/legal/MVG_Cookie_Policy_<ver>.pdf
- /downloads/legal/MVG_DPA_<ver>.pdf
- /downloads/legal/MVG_Subprocessor_Disclosure_Statement_<ver>.pdf
- /downloads/legal/MVG_Security_and_Responsible_Disclosure_Policy_<ver>.pdf
- /downloads/Trust_MeridianVerityGroup.pdf (trust brief)

5. Publishing model (recommended)

- Option 1 (recommended): Extend the existing `MVG_Artifacts_Manifest_*` so `/trust` verification covers legal/trust PDFs automatically.
- Option 2: Publish a separate `MVG_Legal_And_Trust_Docs_Manifest_*` and link it from `/legal` and `/trust`.

Option 1 is highest trust-signal: one verification path, one trust anchor chain.

6. Web integration (copy/paste guidance)

Add the following short callout to `/legal` (and optionally each policy page):

Integrity: These PDFs are included in the Signed Artifacts Manifest (DSSE). Verify via `/trust` – “Verify this site’s verifier”.

Add a link next to each PDF download:

“Verify integrity (Signed Manifest)” – `/trust` (or direct to the manifest JSON).

7. Deployment checklist

- Compute SHA-256 and byte size for each PDF exactly as served.
- Append entries to the artifacts manifest payload, update `generated_utc` and `release_id`.
- Re-sign the DSSE envelope with bootstrap + witness keys (maintain `witness_threshold` policy).
- Update the Release Signature envelope to bind the new manifest hash and path.
- Publish versioned manifest files under `/downloads/`, and (optional) also publish a short-cache “latest” alias.
- Add the new manifest and release signature files themselves to the artifacts manifest (self-referential inventory) if your verifier supports it.

8. HTTP headers (reviewer-friendly)

- For versioned PDFs and versioned manifests: `Cache-Control: public, max-age=31536000, immutable` (safe because versioned).
- For “latest” aliases: `Cache-Control: public, max-age=60–300, must-revalidate`.
- `Content-Type: application/pdf` for PDFs; `application/json` for manifests.
- `X-Content-Type-Options: nosniff`.
- `Strict-Transport-Security` recommended for the site overall.

9. Non-binding note

This manifest posture improves integrity verification for reviewers. Binding legal terms remain those in executed agreements and controlling PDFs. MVG may update publication mechanisms over time; versioned files preserve reproducibility.

Change log

- v1.0.1 — Standardized ASCII hyphenation; added optional timestamping note; condensed layout; clarified PDF/DOCX roles.
- v1.0.0 — Initial publication.