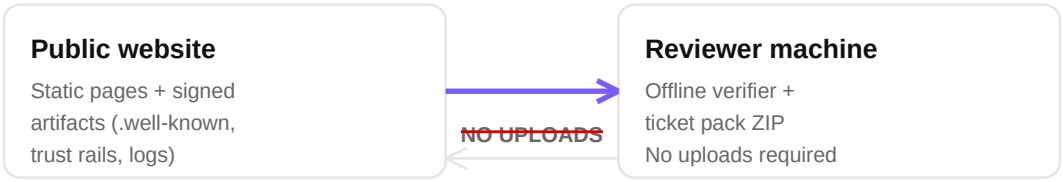
Security Review Packet (Public)

1) Architecture overview (public, redacted)

MVG delivers audit-ready verification as static artifacts and replayable receipts. Reviewers can validate integrity offline without



Key properties

- Offline-first verification (air-gap friendly); no uploads required.
- Fail■closed posture: missing/invalid signatures → HOLD (not GO).
- Evidence is machine-readable (DSSE, receipts, append-only log).
- No third■party scripts or trackers by default.

Disclosure scope (what is intentionally omitted)

- Private keys, key ceremony details, internal network topology, and exploitation playbooks.
- Customer-specific configurations and incident-response runbooks (available under NDA).

Threat model summary

2) Primary threats & mitigations (STRIDE-style summary)

Threat	Primary mitigations
Artifact tampering / substitution	Signatures + sha256 pinning + SRI + offline replay → FAIL/HOLD.
Rollback / replay of older state	Append-only transparency log + prev_root chain + rollback guards.
Partial publication / split-brain release	One-shot publish policy + deterministic status artifacts.
Malicious ZIP / path traversal	Zip-slip safe extraction + strict path normalization in verifiers.
Supply-chain compromise (deps/CI)	Pinned actions + CI gates + deterministic build inputs (SLSA-ready).
Web injection / XSS in verifier UI	Strict CSP, no third-party JS, minimal DOM mutation; offline mode.

Residual risks (public)

- Availability (DNS/CDN) does not affect integrity: verification is offline-replayable.
- Social engineering and endpoint security remain customer responsibilities (shared responsibility).
- For deeper review: request NDA materials (key management, IR runbooks, pen-test summaries).

Evidence pointers

3) Start here — attach 1 URL (DSSE)

```
/.well-known/mvg-procurement-ticket-pack.dsse.json
```

DSSE sha256: 71aaf8e2e1aebed301c266f3c57da05e46b38f0c47e7c78fed318ce9acb93c05
Issued: 2026-02-27T15:59:35Z · Expires: 2026-05-19T16:13:20Z

Transparency log (append-only) — Phase 1.5 chain

Root DSSE: `/transparency/procurement-ticket-pack/prod/root.dsse.json`
Log (NDJSON): `/transparency/procurement-ticket-pack/prod/log.ndjson`
Inclusion proof (LATEST): `/transparency/procurement-ticket-pack/prod/proofs/LATEST.json`
Witness DSSE (Phase 2 scaffold): `/transparency/procurement-ticket-pack/prod/witness/witness.dsse.json`
External anchor receipt (Phase 2 scaffold): `/transparency/procurement-ticket-pack/prod/anchors/LATEST.json`

Artifact chain (index → ZIP → embedded verifier)

Index: /trust/procurement-ticket-pack/MVG_PROCUREMENT_TICKET_PACK_INDEX_PROD_LATEST.json (sha256 3f386e76a1c86ade2a5b77ed8ca0da6422ee0ad8321913c894ed0d6f945976d7)
Ticket Pack ZIP: /downloads/MVG_Procurement_Ticket_Pack_PROD_LATEST.zip (sha256 66325d457ff4a6aced068bca1e3f7ce7a9b144a4e7a0ea60346a1a788e17acd5)
Embedded Verifier ZIP (inside ticket pack): /verifiers/MVG_Public_SiteRelease_Verifier_v50.4.zip (sha256 b09aefb479041e862ccdf0272b2919e9d48c92b6e16cb8eb90ad8a1ce30841be)
Embedded Evidence Bundle ZIP (inside ticket pack): /evidence_bundle/MVG_SiteRelease_Evidence_Bundle_MVG-SITE-PROD-20260218.1.zip (sha256 cc5dd959f108299a03357cc51707fc8d01cd3af6efbd2441d1924cbd536070c7)

Inputs digest (reproducible build marker): b3e21715479188069f63afadb20980c4d58b871b1abec4e8fd4269486e4e287f

Offline verification entrypoints

- Browser-based offline verifier: /verify/ (no uploads, no network required).
- Procurement pass kit: /procurement/ (attachables + expected outputs).
- Site release integrity rail: /trust/site-release/ (DEMO one-shot GO; PROD fail■closed until signed).
- Governance receipt: /.well-known/mvg-governance.json (+ .asc).

Contact & escalation

4) Security contact (RFC 9116 security.txt)

Email: security@meridianverity.com

PGP: https://www.meridianverity.com/pgp.asc
Fingerprint: 94EC 8CD8 863A 2D0C CAF9 2990 B8BF 6577 7FC5 A47F

Responsible disclosure

- Policy: /legal/security-disclosure/ (scope, reporting, safe harbor).
- For urgent issues: prefix subject with [URGENT] and include a secure callback method.
- We coordinate disclosure timelines with reporters in good faith.

Procurement / licensing / legal contacts

Procurement:	procurement@meridianverity.com
Licensing:	licensing@meridianverity.com
Legal:	legal@meridianverity.com
Privacy:	privacy@meridianverity.com

NDA-only materials (available on request)

- Key management & signing ceremony details (HSM/KMS, rotation, revocation).
- Incident response runbooks, audit logs, and access-control models.
- Independent security assessment summaries and remediation tracking.