MVG Procurement Ticket Pack Policy (Public■Safe One■Pager)

Version: 1.0.0 Document ID: MVG-TICKETPACK-POLICY-1.0.0 Classification: Public-safe

Purpose: attachable policy for Security/Counsel to evaluate ticket■pack verification, caching, bootstrap, and rollback semantics.

1) Cache key strategy (branch / environment separation)

Separate DEMO vs PROD at the trust rail level (distinct roots, pointers, and signing roles).
Cache keys MUST include {trust_mode, sequence, sha256} to prevent cross■environment contamination.
Pointers MUST be served with short TTL; verifiers compare sequence + digest before accepting.

2) Bootstrap governance (who / when is allowed)

Bootstrap (reset of pointers / sequences) is a high■trust event and MUST be rare.
Two■person rule: Security Owner + Deploy Operator approve; publish a signed bootstrap event record within minutes.
Allowed reasons: initial go■live, planned key rotation, emergency compromise response, provider migration.
Verifier rule: bootstrap without a signed event record ⇒ HOLD.

3) Rollback guard (monotonic sequence + prev■digest chain)

Ticket Pack Index uses a monotonic sequence. Decreasing sequence ⇒ HOLD.
DSSE pointer includes prev_pointer_digest to create an append■only feel; broken chain ⇒ HOLD.
Rollback is allowed only as a new higher■sequence event with explicit reason codes and signed records.

4) Procurement CI gate (GO■only acceptance semantics)

CI MUST generate the pack, run verify_ticket_pack.py, and allow deploy only on GO.
PROD: missing signatures / partial publication MUST fail closed (HOLD). DEMO: one■shot GO is for external review only.
All attachable artifacts MUST include SHA■256 + bytes; PDF/JSON pointers are discovery metadata, not a substitute for verification.