**OPS-6 — Security drills (pen-test + override trail)**

**Status:** **New**

**Intent**  
Prove security controls work: pen-test fixes, PII masking, override notarization.

**Preconditions**

* RBAC/ABAC in place; tokenization for IDs live.

**Flow**

1. **Pen-test**: external test; track CVEs → fixes → verify retest.
2. **Masking drill**: snapshot non-prod → verify sensitive IDs are masked; attempt exfiltration to confirm block.
3. **Override trail**: perform sample overrides (merge, release) → verify **Notarized Entry** (hash + approver + reason) and end-to-end lineage.
4. **Secrets & keys**: rotate API keys, verify HMAC/webhook signatures after rotation.

**Edge cases**

* Orphan admin accounts → auto-revoke; log incident.
* Webhook replay attempts → verify dedupe.

**Done when**

* All high/med pen-test issues closed; masking verified; override trails complete and queryable.

**Deliverables**  
Pen-test report, masking evidence, override trail report.