**ADD-09 — Config Promotion & Secrets Hygiene (Dev→Stage→Prod)**

**Status:** New

**Intent**  
Promote configs safely between environments; keep secrets clean and rotated.

**Actors**  
Platform Ops • Security • CI/CD

**Preconditions**

* Separate envs; config service; secret manager.

**Flow**

1. **Config Bundles:** versioned, signed bundles per env; diff viewer.
2. **Promotion Gates:** policy checks (lint, schema, referential integrity), approval flow.
3. **Secrets Hygiene:** secret scanning in CI; deny pushes with plaintext secrets; rotations recorded.
4. **Drift Detection:** detect/alert if prod config drifted from approved bundle.
5. **Rollback:** one-click revert to previous approved bundle.

**Edge Cases**

* Emergency patch → fast-track flag with mandatory post-review.
* Partial promotions → block; require all dependencies present.

**Done when**

* Promotions are auditable, gated, and reversible; no plaintext secrets in repo; rotation calendar maintained.

**Deliverables**  
Config bundle repo, promotion runbooks, secret-scan CI rules.