encryption-at-rest-evidence.md

Encryption at Rest — Implementation & Evidence

Purpose

- Document how data-at-rest is protected across services and provide evidence artifacts.

Implementation summary

- Database (Firestore): server-managed encryption at rest is enabled by default. Customer-managed keys (CMK) are used where applicable for production projects (example configuration referenced).
- Backups and snapshots: stored encrypted using the cloud provider's encryption mechanism.
- Secrets: stored in a secrets manager (encrypted at rest) with RBAC enforced.

Evidence provided

- A short screenshot or exported settings file showing encryption-at-rest enabled for the production project (attached as PDF screenshot).
- A dated configuration export or CLI command output indicating encryption is enabled (sample output included in evidence folder).

Review cadence

- Configuration reviewed during quarterly security reviews and after any infrastructure change.

Contact

- security@autopromote.example