Backup Architecture

Design redundant, tamper■evident backups with geographic and vendor diversity, enabling swift recovery without single points of failure.

- Policy on seed splitting vs. Shamir; quorum and custody thresholds.
- Site inventory with access roles and logs.
- Drill schedule for integrity tests.

1) Choose scheme: single■seed with site diversity, split seed, or Shamir (with caution).

2) Create steel backups; label neutrally; record chain type and derivation paths separately.

3) Store in distinct jurisdictions; log seal numbers and custody chains.

4) Test restores on clean hardware; document evidence.

5) Rotate seals and review site controls periodically.

- Avoid complexity that operators can’t execute under stress.
- Don’t co■locate multiple shards; watch for correlated disasters.
- Protect metadata—labels can leak holdings or access hints.

- Steel backup kits; tamper■evident seals
- **Coldcard** for deterministic recovery
- **Nunchuk** for documenting quorum policies

Quarterly integrity checks; annual full restore; site inspection every 6–12 months.