

Wallet Setup & Verification

Deploy wallets with verifiable provenance and correct derivation paths; confirm address correctness before use.

- Trusted hardware wallets (Coldcard + second vendor).
- Clean, offline environment for seed generation.
- Checksum/PGP verification capability for firmware.

- 1) Verify firmware signatures; initialize devices offline.
- 2) Generate seeds; record to steel; never digitize.
- 3) Configure derivation paths (BIP84 native segwit for singlesig; BIP48 for multisig as needed).
- 4) Export xpubs via airgapped method; assemble watch-only wallet.
- 5) Send test transactions; validate receive and change addresses on device.

- Reject devices with evidence of tampering; use supply chain checks.
- Never mix personal and organizational wallets without governance.
- Store xpubs carefully—privacy leaks are cumulative.

- **Coldcard Mk4**
- **Nunchuk Wallet** (derivation/path clarity, multisig coordinator)
- Seed steel backups

Quarterly device health check; validate address derivation after firmware updates; maintain an audit trail.