Incident Response (Loss/Theft/Compromise)

Provide a calm, rehearsed playbook to contain incidents, preserve funds, and restore secure operations.

- Emergency contacts and safe site.
- Pre■built recovery wallet for swift rotation.
- Communication template for stakeholders.

1) Triage: identify scope (lost device, exposed seed, malware, coercion).

2) Contain: freeze hot paths; disconnect compromised devices; move to safe site.

3) Rotate: derive new keys; sweep funds via PSBT with clean devices.

4) Forensics: document indicators; capture evidence; avoid premature disclosure.

5) Post■mortem: root cause analysis; update controls and training.

- Time pressure breeds mistakes—use checklists and two■person confirmation.
- Assume compromised endpoints; perform signing only on trusted hardware.
- Beware extortion/social engineering; coordinate with legal counsel.

- **Coldcard** for rapid key rotation
- **Nunchuk** to coordinate emergency multisig spends
- Offline, pre■prepared recovery wallet

Annual live■fire simulation; quarterly tabletop exercise; refresh contact lists every 6 months.