

BEGINNER DOWNLOAD 03

Wallet Setup and Recovery Checklist

Plan the wallet, create it privately, protect the recovery material and verify that access can be restored before meaningful funds are added.

**THE
CONTROLLING
PRINCIPLE**

Anyone with the recovery phrase or private key may be able to control the assets. Legitimate support does not need either one.

1. Define the wallet's purpose

- ☐ I identified whether this wallet is for long-term storage, routine transactions, DeFi, business activity or testing.
- ☐ I decided whether custodial or self-custodial control is appropriate for the purpose.
- ☐ I understand who controls the keys and who can recover, freeze or approve transactions.
- ☐ I confirmed the exact networks, assets and applications the wallet must support.
- ☐ I am using a separate wallet for unfamiliar applications rather than exposing long-term holdings.

2. Obtain and prepare safely

- ☐ I obtained the device or application from the manufacturer or another verified source.
- ☐ I checked the publisher, website address, packaging and device condition.
- ☐ The computer or phone is updated, protected and free of untrusted remote-access software.
- ☐ I am creating the wallet in a private place without cameras, screen sharing or other people present.
- ☐ No person supplied a prewritten recovery phrase, initialized device or wallet file.

3. Create and secure the wallet

- ☐ The wallet generated the recovery material during my own trusted setup process.
- ☐ I set a strong PIN or password that is not reused elsewhere.
- ☐ I enabled appropriate device security and multifactor authentication for related custodial accounts.
- ☐ I recorded the wallet name, purpose, networks and date created without recording secrets in this checklist.
- ☐ I verified the first receiving address on the trusted wallet or hardware display.

**NEVER
PHOTOGRAPH
THE PHRASE**

Do not store recovery words in ordinary photos, email, cloud notes, chat, password hints or online forms.

RECOVERY PLAN

Back Up. Verify. Separate. Test.

A backup is useful only when it is accurate, available to the authorized owner and protected from theft, damage and accidental disclosure.

4. Protect the recovery material

- ☐ I recorded every recovery word accurately, in the correct order, using a durable offline method.
- ☐ The backup is stored separately from the wallet device and protected from fire, water, theft and casual discovery.
- ☐ No single unauthorized person can access both the device and its recovery material.
- ☐ Additional copies, passphrases or shared arrangements are documented without creating an unusable level of complexity.
- ☐ I understand that a wallet passphrase can create a different wallet and may be unrecoverable if forgotten.

5. Verify recovery before funding

- ☐ I used the wallet's trusted verification procedure to confirm the recovery words.
- ☐ When appropriate, I completed a controlled recovery test before adding meaningful funds.
- ☐ The restored wallet produced the expected addresses or balances.
- ☐ I did not enter recovery words into a website, support chat or unsolicited application.
- ☐ I sent a small test transaction and confirmed receipt on the correct network.

6. Continuity and review

- ☐ An authorized person can locate clear recovery instructions after incapacity, death or staff turnover.
- ☐ The plan explains the wallet type, required devices, backup locations and approval process without unnecessarily exposing secrets.
- ☐ I scheduled periodic reviews of devices, backups, software support and authorized access.
- ☐ I know how to move assets to a new wallet if a device, phrase or key may be compromised.

Non-secret wallet record

Use this table only for operational information. Never enter a recovery phrase, private key, PIN, password or hidden passphrase.

Wallet name / purpose	
Wallet type	
Supported networks	
Date created	
Device / software	
Backup verified date	
Next review date	