# Three-Wallet Toolkit

Practical worksheets and checklists for setting up and maintaining your Three-Wallet Model®

*Companion to The Three-Wallet Model®: A Practical Guide, 2026 Edition*

**Crypto Safety First**

CryptoSafetyFirst.com

# Your Three-Wallet Model® at a Glance

The Three-Wallet Model® separates your crypto activity across three wallets with different purposes and levels of exposure.

The goal is simple: do not expose everything you own to the same risks.

## Vault Wallet

**Purpose:** Long-term storage and maximum protection.

Use your Vault for crypto assets you do not need for regular transactions.

**Setup essentials**

- Use a hardware wallet.
- Buy the device directly from the manufacturer's official store. Never use a device that arrives set up, with a PIN or with a recovery phrase supplied.
- Check the packaging and device for signs of tampering.
- Store your seed phrase securely offline.
- Keep more than one protected physical backup for important holdings.
- Complete a recovery test **before funding the Vault**.
- If you use a passphrase, include it in your recovery planning.
- No legitimate support agent, website or unexpected prompt will ever ask for your seed phrase – anyone who does is a scammer. Enter a hardware wallet's phrase only on the device itself.

**Keep your Vault isolated:**

Do not connect the Vault directly to dApps or use it for routine transactions.

## Frequent Use Wallet

**Purpose:** Regular crypto activity with controlled exposure.

Use it for routine transfers, established dApps and other regular Web3 activity.

**Setup essentials**

- Keep only the amount needed for regular activity.
- Back up the seed phrase securely.
- Keep trusted addresses in an address book where supported.
- Never copy a destination address from transaction history.
- Read what you sign.
- Review and revoke token approvals you no longer need.

**Think of it as your working wallet:**

It should contain enough for normal activity, but not your long-term holdings.

## Disposable Wallet

**Purpose:** Isolate higher-risk or temporary activity.

Use it for unfamiliar dApps, new mints, airdrops and other interactions where you want additional separation from your main wallets.

**Setup essentials**

- Keep only the amount needed for the intended interaction.
- Read what you sign.
- Avoid unnecessary or unlimited token approvals.
- Revoke approvals after the interaction when appropriate.
- Replace the wallet when its purpose is complete or after untrusted exposure.

**Remember:**

A Disposable Wallet can limit what is exposed. It does not make a risky transaction safe.

## The Model in One Line

Vault → protect | Frequent Use → transact | Disposable → isolate

The strength of the Three-Wallet Model® comes from keeping these roles separate and maintaining them over time.

# Wallet Metadata Log

Use this log to keep track of your wallets without recording sensitive recovery information.

Never write your seed phrase, private key, PIN or passphrase in this log.

## Wallet Information

| Wallet Label | Wallet Type | Public Address (full) | Device / Wallet | Chain(s) |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

## Recovery & Purpose Record

| Wallet Label | Purpose | Creation Date | Backup Type | Backup Location |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

## Connections & Approvals

| Wallet Label | Connected dApps / Tools | Active Token Approvals | Last Reviewed |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

## Security Reminder

Store this log separately from your backups. Describe backup locations so only you and your heirs understand them.

Do not record information that could be used to access or recover your crypto, including seed phrases, private keys, PINs or passphrases.

# Backup Planning Table

Use this worksheet to document **how your wallet backups are protected and where they are stored**. Do not write the seed phrase, private key or passphrase itself in this table. Multisig: also note where the wallet configuration file (descriptor) is backed up – the keys alone may not restore the wallet.

| Wallet | Backup Goal | Storage Method | Number of Backups | Backup Location(s) | Last Checked |
|---|---|---|---|---|---|
| Vault | Protect long-term access and recovery | | | | |
| Frequent Use | Maintain secure recovery access | | | | |
| Disposable | Recovery only if needed for its intended use | | | | |

## Backup Review

For each important wallet, confirm:

1. I know where the backup is stored.
2. The backup is readable and physically protected.
3. Important wallets have more than one protected physical backup.
4. Backup copies are not stored together where one incident could destroy or expose all of them.
5. I have not stored seed phrases or private keys in this Toolkit.
6. My recovery information is understandable to the person who may need it in an emergency.

## Important

A backup only helps if it works when you need it. Keep it protected, accessible when legitimately needed, and check it regularly. Keep more than one protected physical backup for important wallets.

# Quarterly Maintenance Checklist

Complete this checklist **every three months** to keep your Three-Wallet Model® organized and secure.

| Check | Action | Completed |
|---|---|---|
| Backup inspection | Check that wallet backups are still readable, secure and stored in their intended locations. | ☐ |
| Token approvals | Review active token approvals and revoke permissions you no longer need. | ☐ |
| Wallet software | Update wallet apps, browser extensions and mobile apps to the latest versions from the official store. | ☐ |
| Hardware wallets | Check for relevant firmware updates and obtain them only through official channels. | ☐ |
| Disposable wallets | Review Disposable wallets and retire those that are no longer needed or have completed their intended purpose. | ☐ |
| Security advisories | Check official security notices for the wallets, devices and services you use. | ☐ |
| Security hygiene | Review your wallet practices and correct any habits that have increased unnecessary exposure. | ☐ |
| dApp connections | Disconnect your wallets from dApps you no longer use. | ☐ |

## Quarterly Review Record

| Review Date | Issues Found | Actions Taken | Next Review |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |

**Important:** Install wallet apps, browser extensions and updates only from official sources.

# Semiannual Maintenance Checklist

Complete this checklist **every six months** to make sure your Three-Wallet Model® still reflects how you actually use your crypto.

## Six-Month Review

| Check | Action | Completed |
|---|---|---|
| Wallet inventory | Review your wallet inventory and confirm that each wallet is still correctly identified and labeled. | ☐ |
| Wallet purpose | Confirm that each Vault, Frequent Use and Disposable wallet is still being used for its intended purpose. | ☐ |
| Metadata log | Update your Wallet Metadata Log with any wallets created, replaced or retired since the previous review. | ☐ |
| New wallets | Make sure any new wallets have been properly documented and backed up where required. | ☐ |
| Inheritance readiness | Review whether a trusted person could locate and understand the information needed in an emergency without unnecessarily exposing your assets today. | ☐ |

## Six-Month Review Record

| Review Date | Changes Needed | Actions Taken | Next Review |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

# Annual Maintenance Checklist

Complete this checklist once a year to confirm that your Three-Wallet Model® remains recoverable, properly documented and appropriate for your current situation.

## Annual Review

| Check | Action | Completed |
|---|---|---|
| Recovery process | Walk through a complete recovery process to confirm that your recovery plan is clear and usable – for a hardware wallet only on the device itself (built-in backup check), never by typing the recovery phrase into a phone, computer, website or app. | ☐ |
| Backup locations | Review your backup locations and confirm that they remain secure, accessible when legitimately needed and appropriately separated. | ☐ |
| Life changes | Consider whether changes in your family, residence or personal circumstances require updates to your recovery or inheritance arrangements. | ☐ |
| Unused wallets | Identify wallets that are no longer needed and determine whether they should be retired. | ☐ |
| Devices | Review old or unused hardware devices and make sure they do not create unnecessary security or recovery risks. | ☐ |
| Vault allocation | Confirm long-term assets are in the Vault, not in Frequent Use or Disposable wallets. | ☐ |
| Documentation | Update your wallet records, backup information and inheritance documentation where necessary. | ☐ |

## Annual Review Record

| Review Date | Changes Needed | Actions Taken | Next Annual Review |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

## Recovery Reminder

A recovery plan should work before an emergency happens. Your annual review is the opportunity to confirm that your documentation, backups and recovery arrangements still match your actual wallet setup.

Never record seed phrases, private keys, PINs or passphrases in this Toolkit.

# If a Wallet Is Compromised

Act quickly, but don't rush into new mistakes. Work through these steps in order, from a device you trust.

## 1. Stop the damage

- Stop interacting with the website, app or contract involved. Close it and disconnect your wallet.
- Don't sign anything else until you know what happened.
- If you suspect malware, stop using that computer or phone for crypto. Use a clean device for the steps below.

## 2. Work out what was exposed

| What happened | What it means |
|---|---|
| You signed a malicious approval or transaction | Treat the wallet as compromised: some signatures (account delegations, owner or permission changes) give the attacker full control, not just the approved tokens. |
| You entered your seed phrase on a website or in an app, or shared it | The wallet is permanently compromised, and so is every account created from that seed phrase. |
| Your device may be infected | Treat every software wallet on that device as compromised. |

## 3. Protect what's left

- **Malicious approval or signature: first move the remaining funds to a new wallet with a new seed phrase. Revoke approvals on the old address only if you must keep using it.**
- **Seed phrase exposed or device infected:** create a new wallet with a new seed phrase on a clean device. Move any remaining assets there. Never use the old seed phrase again.
- Don't send funds into a compromised wallet to pay fees. Automated bots can take them within seconds.
- **Your Vault:** a hardware wallet stays safe as long as its seed phrase was never typed or stored on the affected device. Still, confirm every action on the device screen. If the Vault's seed phrase was ever exposed, move its assets to a new Vault.
- **Disposable wallet:** abandon it. Don't reuse it.

## 4. Secure your accounts

- From a clean device, change the passwords for your exchange and email accounts, and check their 2FA settings.
- Check your exchange accounts for unknown withdrawal addresses or logins.

## 5. Record and report

- Note the date, the wallet addresses involved, the transaction IDs, and the websites or contacts used. Take screenshots.
- If the funds went to an exchange, contact that exchange right away with the transaction IDs. It may be able to freeze them.
- Report the theft to the police or your national cybercrime reporting service.

## 6. Beware of recovery scams

After a loss, scammers often contact victims and offer to get the funds back: "recovery experts", fake lawyers, fake authorities or "blockchain investigators".

- No one can reverse a blockchain transaction for you for a fee.
- Never pay upfront for recovery, and never share your seed phrase.
- Treat anyone who contacts you first after your loss as a scammer unless you verify them through official contact details – real police or exchanges never ask for fees, crypto or your seed phrase.

## 7. Rebuild

- Set up fresh wallets following the Three-Wallet Model®, and update your Wallet Metadata Log.
- Write down what happened and what you'll do differently.

© 2025–2026 Juan Pablo Renedo. All rights reserved. Free to share in its complete, unmodified form. Three-Wallet Model® is a registered EU trademark of Juan Pablo Renedo.

Published by Juan Pablo Renedo, c/o Block Services, Stuttgarter Str. 106, 70736 Fellbach, Germany · contact@cryptosafetyfirst.com

Educational information only – not financial, tax or legal advice. To the extent permitted by law, no liability is assumed for losses resulting from its use; this does not apply to intent, gross negligence or injury to life, body or health.