SETUP GUIDE

Hardware Wallet and Signing Device Setup Guide for Web3 Teams

Generating, protecting, and operating hardware signers

Prepared for	Web3 team members	Classification	Internal
Prepared by	Oak Security	Date	2026-06-17

Oak Security GmbH

1. What This Guide Is For

This guide is for anyone in a Web3 team who holds non-trivial value or acts as a signer, whether you are a developer, an operator, a treasury signer, or in a non-technical role with access to funds. A hardware wallet (signing device) keeps your private keys inside a dedicated device so that a compromised laptop or phone cannot extract them or sign on your behalf. That protection only holds if the device is set up and operated correctly.

The aim is not to make every signer identical. The aim is to keep a normal endpoint problem, such as malware on a laptop, a malicious dApp, a swapped clipboard address, or a phishing prompt, from turning into a drained wallet or a treasury loss.

> **NOTE**
>
> **Baseline rule:** the seed never exists in digital form, you verify every address and transaction on the device screen, firmware comes only from the official vendor app, and backups stay offline.

For the most sensitive roles, such as treasury signing, cold storage, and multisig participation, a stronger setup applies: a passphrase, a dedicated device per role, an air-gapped signer, and physical separation of the seed from the passphrase. Section 8 covers those rules.

2. Choosing a Device and Threat Model

A hardware wallet defends the private key against a compromised host. It does not defend against everything. Pick the device class against the threats your role actually faces, not against convenience.

Device Class	Example Devices	Protects Against	Weakness
USB hardware wallet	Ledger, Trezor	Key extraction by host malware, since signing happens on-device. Convenient for frequent signing.	Connected to a possibly compromised host over USB. Relies entirely on you verifying address and transaction on the device screen.
Air-gapped signer (QR / microSD)	Keystone, Coldcard	Everything above, plus no USB data path to the host. Transactions cross an air gap by QR code or microSD, so host malware cannot talk to the device directly.	More steps per signature. microSD and QR handling still need discipline. Firmware and supply chain still matter.
Dedicated single-purpose signing laptop	A clean, offline machine used only for signing	Useful where a hardware wallet is not supported for a chain or tooling. Reduces blast radius by isolating signing from daily work.	A general-purpose OS is a far larger attack surface than a hardware wallet. Only as good as its isolation and update discipline.

What Each Threat Means

- **Malware on the host.** Keyloggers, clipboard hijackers, and malicious browser extensions. A hardware wallet keeps the key off the host, but a swapped destination address only gets caught if you verify it on the device screen.

- **Supply-chain compromise.** A device tampered with before it reaches you, or a pre-loaded seed. Defeated by buying from the vendor or an authorized reseller and running the genuine-device check.
- **Physical theft.** Someone takes the device. Defeated by a PIN and, for higher value, a passphrase. Without a passphrase, the seed backup alone is enough to drain funds.

Vendor Selection and the Genuine-Device Check

Buy only from the vendor directly or an authorized reseller listed on the vendor site. Every major vendor provides a genuine-device check: Ledger devices attest through Ledger Live, Trezor through Trezor Suite, Keystone and Coldcard through their documented verification steps. Run it before you trust the device with any value. A device that fails or cannot complete the check is not used.

3. Quick Setup Checklist

Every signing device needs these steps before it holds value.

Device Setup

Step	What To Do
Source	Buy from the vendor or an authorized reseller only. Never second-hand or from a general marketplace.
Genuine check	Run the vendor genuine-device check in the official app before use.
Firmware	Update to the latest firmware through the official vendor app before generating the seed. Later updates through the official app are safe and expected.
Initialize	Let the device generate a new seed on-device. Never import or accept a provided seed.
PIN	Set a non-trivial PIN. Do not reuse a phone unlock code or a memorable date.
Passphrase	For treasury and high-value roles, enable a BIP-39 passphrase (hidden wallet).

Backup and Verification

Step	What To Do
Write the seed	Write the recovery words on paper or metal, offline, by hand. Never photograph or type them anywhere digital.
Verify the backup	Complete the device-prompted backup check so you know the words are correct.
Verify an address	Generate a receive address and confirm it matches on the device screen before funding.

Test transaction	Fund with a small amount, send it back, and verify the destination on-device before approving.
Store offline	Keep the backup offline and, for higher value, geographically separated and split.

4. Initialization and Seed Generation

The seed (recovery phrase) is the wallet. Anyone who has it controls the funds, with no device and no PIN required. This section covers generating the seed securely and keeping it off any digital system.

Generate on the Device

Let the device generate the seed using its own hardware entropy. Do not import a seed you generated elsewhere, do not accept a seed printed on a card, and do not accept a device that is already initialized. A pre-set seed is the classic supply-chain attack: the attacker keeps a copy and waits for you to fund it.

Run the genuine-device check before you generate anything. The check confirms the device is running authentic vendor firmware and is not a counterfeit or a tampered unit.

PIN Policy

Set a PIN that is not a phone unlock code, a birth year, or a repeated digit. The PIN protects against casual physical access: it slows a thief who steals the device, buying you time to move funds to a new wallet using your seed backup. You can move funds at any point with the backup, lost device or not. The PIN protects nothing if the seed backup is sitting next to the device.

Wrong-PIN behavior is vendor-specific, so do not assume the device wipes itself. Ledger wipes after three wrong attempts; Trezor allows more, with an escalating delay. Coldcard does not auto-wipe by default and instead relies on a long PIN, a login countdown, and optional duress/brick PINs. Because you cannot count on a wipe, use a long, non-guessable PIN, especially on devices that do not auto-wipe.

Optional Passphrase (Hidden Wallet)

A BIP-39 passphrase is an extra secret added on top of the seed. It produces an entirely separate wallet (a hidden wallet). The seed plus the passphrase together control the funds. The seed alone controls nothing of value.

- For treasury and high-value roles, a passphrase is mandatory (see Section 8).

- The passphrase is not stored on the device. If you forget it, the funds are gone. There is no recovery.
- Store the passphrase separately from the seed, never together. Whoever holds both holds the funds.
- Treat the passphrase with the same care as the seed: never digital, never photographed, never typed into a website.

Write the Seed Offline and Verify It

Write the recovery words by hand, offline, on paper first and then transfer to metal (Section 5). Then complete the backup-verification step the device prompts for. This step has you re-enter or confirm the words so that a transcription error does not surface later as an unrecoverable wallet. A backup you never verified is a backup you do not have.

5. Seed Backup and Recovery

The backup is the single point of failure for the whole wallet. It must survive fire, water, loss, and theft, and it must never appear in any digital system.

Backup Medium and Distribution

- **Metal backup.** Paper degrades and burns. Use a metal seed backup (stamped or tiled) for anything beyond trivial value.
- **Geographic distribution.** For high value, do not keep the only backup in the same building as the device. A single fire or burglary should not end both.
- **Single seed vs. split.** A single-seed backup is simple but is a single object an attacker needs to steal. A Shamir / SLIP-39 split divides the secret into shares where a threshold (for example, 2-of-3) reconstructs it, so no single location is sufficient. Use Shamir for high-value or shared-custody seeds; keep single-seed only for lower-value, single-holder wallets. Caveat: SLIP-39 is a different standard from the BIP-39 12/24-word phrase and is effectively Trezor-only. Its shares are not interchangeable with a BIP-39 word backup and cannot be restored on a Ledger, Keystone, or Coldcard. If you Shamir-split, your recovery device must support SLIP-39, and the dry-run in Step 6 must use such a device. For team treasuries, prefer multisig over splitting a single seed.
- **Passphrase stored separately.** If you use a passphrase, store it in a different location from the seed and from any single Shamir share. The point of the passphrase is defeated if it sits next to the seed.

Decoy / Duress Wallet

The passphrase mechanism lets you maintain a decoy wallet: the no-passphrase wallet (or a low-value passphrase) holds a small, plausible balance, while the real funds live behind a separate passphrase. Under coercion you can surrender the decoy. Fund the decoy with enough to be believable. Caveat: hidden wallets are well documented, so deniability is weak against an informed coercer who knows to ask for a passphrase. Do not treat the decoy as a reliable defense against targeted physical coercion, and avoid linking the decoy wallet to your main identity through on-chain activity.

Continuity and Inheritance

Decide in advance who can recover funds if the holder is unavailable, and document the recovery procedure without writing the secret into the document. For team treasuries this is usually solved by multisig rather than by sharing a single seed (see the multisig guide). For individual high-value holdings, a Shamir split with shares held by trusted parties or in separate secure locations is the common pattern.

Absolute Rules

- Never photograph the seed or passphrase.
- Never type the seed or passphrase into any website, app, form, or "wallet validation" / "wallet sync" prompt. No legitimate service ever asks for it.
- Never store the seed or passphrase in cloud storage, Notes, password managers, screenshots, email, chat, or any file.
- Never read the seed aloud near a phone, a smart speaker, or in a video call.

6. Operating the Device Safely

The device protects the key. It cannot protect you from approving a transaction you did not read. Most hardware-wallet losses are not key extraction; they are users approving malicious transactions or sending to attacker-controlled addresses.

Firmware Updates

Update firmware only through the official vendor app (Ledger Live, Trezor Suite, Keystone or Coldcard tooling). The app verifies the firmware signature against the vendor key. Do not apply firmware from a link in an email, a chat, a pop-up, or a third-party site. A "critical firmware update" delivered by email is a phishing pattern. Keep firmware current: ignored updates leave known vulnerabilities in place.

Verify Receive Addresses On-Device

Before funding or sharing a receive address, display it on the device screen and confirm it matches what the host shows. Clipboard-hijacking malware swaps the address shown on the host. The device screen is the only display the malware cannot touch.

Clear Signing vs. Blind Signing

- **Clear signing** shows the actual transaction details (recipient, amount, contract call, parameters) on the device screen so you can verify what you are approving.
- **Blind signing** approves a hash or opaque payload that the device cannot decode and display in human-readable form. You are trusting the host to have shown you the truth, which defeats the purpose of the device.

Keep blind signing disabled. Enable it only for the specific operation that requires it, verify the context independently, and disable it again afterward. Blind signing was the mechanism behind several large losses where a signer approved an opaque payload that drained an account or altered approvals. If a dApp demands blind signing for a routine action, treat that as a red flag.

Connecting to dApps

- Connect only through the official vendor app or a wallet you trust, on the work browser profile.
- Read what you are signing on the device. Token approvals (especially unlimited approvals), `setApprovalForAll`, and permit signatures grant ongoing access, not a one-time transfer.
- Revoke stale approvals periodically.
- Treat any unexpected signing prompt as hostile until you understand exactly what it does.

Using the Device as a Multisig Signer

A hardware wallet can act as one signer in a multisig. This is the recommended pattern for team treasuries: no single device or person can move funds alone, and a single compromised signer does not end the treasury. Setup, threshold policy, and signer separation are covered in the separate multisig guide. The device-level rules in this guide (genuine check, on-device verification, no blind signing) apply to every multisig signer.

7. The Recommended Setup Flow

Step 1: Acquire from the Vendor

Buy the device directly from the vendor or an authorized reseller listed on the vendor site. Do not buy second-hand, from a general marketplace, or from a third party offering a discount. Inspect the packaging for tampering on arrival.

Step 2: Verify Genuine and Update Firmware

Install the official vendor app from the vendor site. Run the genuine-device check. Only after it passes, apply any pending firmware update through the app, before you generate the seed. Updating firmware later, after the wallet is in use, is safe and expected when done through the official app (the device preserves the seed; on some Trezor models a fresh-device firmware install wipes a device that has no seed yet, which is fine before initialization). If the genuine check fails, stop and contact the vendor; do not use the device.

Step 3: Initialize and Set a PIN

Let the device generate a new seed on-device. Do not import or accept any provided seed. Set a non-guessable PIN that you do not reuse from a phone or a memorable date.

Step 4: Decide on a Passphrase

For treasury and high-value roles, enable a BIP-39 passphrase now and plan to store it separately from the seed. For lower-value personal use, a passphrase is optional but adds protection against backup theft. If you enable one, understand there is no recovery if you forget it.

Step 5: Back Up the Seed to Metal

Write the recovery words by hand, offline, then transfer to a metal backup. For high value, plan geographic distribution and consider a Shamir / SLIP-39 split. Store the passphrase, if any, in a different location.

Step 6: Verify Recovery

Complete the device-prompted backup verification so you know the words are correct. For high value, perform a full dry-run recovery onto a spare device or by wiping and restoring, then confirm the same addresses appear. When comparing, check the same derivation path and account index, and remember that a passphrase produces entirely different addresses: a dry-run that compares the wrong account or omits the passphrase will look like a failed recovery when the backup is actually fine.

Step 7: Fund a Test and Verify an Address

Generate a receive address and confirm it on the device screen. Send a small test amount, then send it back, verifying the destination on-device before approving. Only then move meaningful value.

Step 8: Enroll as a Signer Where Applicable

If the device is a multisig signer, enroll its address into the multisig per the multisig guide, confirm the on-device address matches what the multisig records, and verify your signer role with a small test transaction before relying on it.

8. Extra Rules for Critical-Access Users

Treasury signers, cold-storage holders, and anyone who can move significant value face a higher bar. A single compromise here is a company-level incident.

Control	Requirement
Passphrase	Mandatory. The seed alone must not control any meaningful value.
Dedicated device per role	Do not reuse one device across treasury, personal, and testing. A dedicated device per role limits blast radius and avoids cross-contamination.
Air-gapped cold storage	Hold long-term reserves on an air-gapped (QR / microSD) signer, not on a USB device used for daily signing.
Seed and passphrase separation	Store the seed and the passphrase in different locations. Whoever holds both controls the funds.
No single person holds both	No individual should hold both the seed and the passphrase for a treasury wallet. Split custody or use multisig.
Geographic separation	Distribute seed backups (or Shamir shares) across separate physical locations so one event cannot destroy or steal all of them.
Multisig	Prefer multisig over a single signer for team treasuries, so no single device or person can move funds alone.
Blind signing	Disabled by default. Enabled only for a specific, independently verified operation, then disabled again.
Travel	Do not travel with the device, its seed backup, and its passphrase together. Separate them, or leave cold-storage material at home.

Suspicious activity	Stop signing and escalate before resuming. Move funds to a freshly generated wallet if exposure is plausible.

9. Things To Avoid

These habits are common and each one has cost teams real funds.

- Buying a device second-hand or from a general marketplace instead of the vendor or an authorized reseller.
- Accepting a pre-initialized device, or using a seed that came printed on a card or sent to you.
- Storing the seed or passphrase on a phone, in cloud storage, in a password manager, in Notes, or as a photo.
- Entering a seed or passphrase into any website, app, or "wallet validation," "wallet sync," or "security update" prompt.
- Approving transactions without reading the recipient, amount, and contract call on the device screen.
- Blind-signing opaque payloads as a matter of routine.
- Reusing one device across treasury, personal, and test wallets.
- Storing the seed and the passphrase in the same place.
- Ignoring firmware updates, or applying firmware from a link instead of the official vendor app.
- Trusting a host-displayed receive address without confirming it on the device screen.
- Granting unlimited token approvals or `setApprovalForAll` to dApps and never revoking them.

10. If Something Suspicious Happens

If you suspect the seed has been exposed, the device has been tampered with, or you approved a transaction you should not have, treat the wallet as compromised. A seed cannot be "un-exposed." The only safe action is to move funds to a new wallet generated on a clean device.

Immediate

1. Stop signing. Do not approve anything else on the suspect device.
2. If funds are still present and movable, prepare to move them to a new wallet (below) before an attacker does.
3. Note what happened: what you saw, what you approved, what prompt you answered. This helps the team assess scope.
4. Notify the security owner or treasury lead from a trusted channel.

Contain

- If the device may be physically tampered with, stop using it entirely.
- If you entered the seed or passphrase into anything digital, assume both are now known to an attacker.
- If you approved a token approval or `setApprovalForAll`, revoke it immediately, and assume the attacker may act before the revocation lands.

Rotate

5. Generate a new seed on a clean, genuine, verified device (Sections 4 and 7).
6. Move all funds from the suspect wallet to the new wallet.
7. Treat the old seed as burned: never reuse it, never re-fund it, even if nothing was lost yet.
8. Re-enroll the new signer in any multisig, and remove the old signer.
9. Revoke any dApp approvals tied to the old wallet.

Rebuild

- Set up the replacement device fully per Section 7, including a new metal backup and, for critical roles, a new passphrase stored separately.
- If you have treasury access, do not resume signing until the security owner agrees the new setup is clean.
- Review how the exposure happened (phishing, malware, a bad prompt, physical access) and close that gap before resuming.

11. Quarterly Self-Check

Once a quarter, do this short review.

Check	Done
Device firmware is current, applied only through the official vendor app.	
The seed exists only offline, on metal, never in any digital form.	
The seed backup is stored offline and, for high value, geographically separated.	
The passphrase, if used, is stored separately from the seed.	
No single person holds both the seed and the passphrase for a treasury wallet.	
Blind signing is disabled except for specific, verified operations.	
Receive addresses are verified on the device screen before funding.	
Stale dApp token approvals have been reviewed and revoked.	
Treasury and high-value roles use a dedicated device and a passphrase.	
A recovery dry-run has been performed for high-value backups.	
Devices are not traveled with alongside their seed and passphrase.	
Multisig signers match the on-device addresses on record.	

12. References

- Ledger support (device setup, Genuine Check, firmware): https://support.ledger.com/
- Trezor setup and security: https://trezor.io/learn
- Keystone setup and verification: https://support.keyst.one/
- Coldcard quick start and verification: https://coldcard.com/docs/quick/
- Coldcard firmware verification: https://coldcard.com/docs/upgrade/
- BIP-39 (mnemonic seed phrases): https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki
- BIP-39 passphrase guidance (Trezor): https://trezor.io/learn/a/passphrases-and-hidden-wallets
- SLIP-39 (Shamir secret sharing): https://github.com/satoshilabs/slips/blob/master/slip-0039.md
- Revoke token approvals (vendor-neutral): https://revoke.cash/