A SEED PHRASE IS NOT AN INHERITANCE PLAN.

The Crypto Inheritance Readiness Checklist

A practical, security-first workbook for hardware-wallet owners who want their family to have a process without exposing access today.

NO SEED PHRASE / NO WALLET ADDRESS / NO BALANCE

Digital Asset Legacy

Edition 1.0 | Educational use only

Before you write anything

This workbook is designed to document a process, not the credentials that control your assets. Complete it without copying private access information into this file.

Never type or paste a recovery phrase, private key, passphrase, PIN, wallet address, balance, device serial number, or exact storage location into this document or any online form.

The three-layer rule

1 MAP	What exists, who is responsible, and where approved instructions are held. No secrets.
2 INSTRUCT	What trusted people should do, whom they should contact, and what they should avoid.
3 ACCESS	Recovery material remains offline and separately protected according to your own threat model.

Scope and disclaimer

This checklist provides general educational information. It is not legal, tax, investment, cybersecurity, or estate-planning advice. Laws, wallet designs, custody arrangements, and tax treatment vary. Work with qualified professionals in your jurisdiction, and test any recovery process using a low-risk environment before relying on it.

Your 10-point readiness check

Check only what is true today. Each checked item is one point.

- ☐ I maintain a current, non-secret inventory of the digital-asset systems I use.
- ☐ At least one trusted person knows that an inheritance process exists.
- ☐ My legal documents address digital assets where appropriate.
- ☐ My recovery material is stored offline and protected from a single point of failure.
- ☐ Instructions and recovery material are not stored together in one easily compromised place.
- ☐ My family knows whom to contact before attempting any wallet recovery.
- ☐ The plan explains devices, software, and dependencies without revealing credentials.
- ☐ I have tested the process without exposing or moving meaningful assets.
- ☐ I have considered incapacity as well as death.
- ☐ I review the plan after major wallet, family, legal, or geographic changes.

SCORE	STATUS	NEXT MOVE
0-3	Fragile	Start with inventory and trusted-person awareness.
4-7	Developing	Close the gaps and run a safe rehearsal.
8-10	Prepared	Schedule reviews and confirm professional alignment.

Build a non-secret inventory

The goal is discoverability, not access. Use categories and references that make sense to your executor without revealing values or credentials.

SYSTEM OR CATEGORY	ARRANGEMENT	EVIDENCE / RECORD LOCATION	LAST REVIEW
	Hardware wallet / custodian / multisig / other		
	Hardware wallet / custodian / multisig / other		
	Hardware wallet / custodian / multisig / other		
	Hardware wallet / custodian / multisig / other		
	Hardware wallet / custodian / multisig / other		
	Hardware wallet / custodian / multisig / other		
	Hardware wallet / custodian / multisig / other		

SAFE INVENTORY EXAMPLE: 'Primary self-custody wallet. Device instructions are held with estate documents. Recovery material is stored separately.'

Do not record

Balances, public addresses linked to your identity, seed words, private keys, PINs, passphrases, serial numbers, exact hiding places, or photographs of recovery material.

Assign people, not just documents

A resilient plan separates decision-making, technical help, legal authority, and access. One person does not need to know everything.

ROLE	PERSON / FIRM	WHAT THEY KNOW	BACKUP
Legal decision-maker		Authority, documents, timing	
Trusted family contact		That a plan exists and first steps	
Technical guide		Approved process and device context	
Tax professional		Records and reporting workflow	
Contingency contact		Who steps in if someone is unavailable	

Contact protocol

The first person to contact

The first professional to contact

A person who must not act alone

Where current contact details are maintained

Design for the day when somebody is stressed, grieving, and unfamiliar with your setup. Clear sequencing is a security control.

Family emergency letter template

Keep this letter free of secrets. Its purpose is to slow people down and direct them to the approved process.

If I am unable to manage my digital assets, do not enter recovery words into a website, share photographs of wallet materials, accept unsolicited help, or move assets before confirming the approved process.

The person who should coordinate	
The legal document to locate	
The professional to contact	
The non-secret inventory is located	
The instructions were last reviewed	

What I want you to know

Signature / date: ____

Separate explanation from access

A single package containing instructions and recovery material can become a single point of failure. Map the layers without recording their precise locations here.

LAYER	CONTAINS	AVAILABLE TO	REVIEW TRIGGER
Estate documents	Authority and beneficiary intent	Attorney / executor	Family or legal change
Process instructions	Sequence, contacts, dependencies	Approved trusted people	Wallet or process change
Recovery material	Offline access material	Only under your chosen controls	Storage or threat-model change
Verification record	Evidence a rehearsal occurred	Plan owner / reviewer	After every rehearsal

Dependency check

- ☐ Required device or compatible replacement path is documented.
- ☐ Required software name and official source are documented.
- ☐ Passphrase dependencies are accounted for without exposing them.
- ☐ Multisignature participants and quorum rules are understood.
- ☐ Instructions work if a specific person, company, or device is unavailable.

Run a safe rehearsal

Do not wait for an emergency to discover a missing dependency. Rehearse the communication and decision process without exposing live credentials or moving meaningful assets.

01	Tabletop walkthrough Ask the trusted person to explain the first five actions using only the written process.
02	Contact verification Confirm that professional and family contacts are current and understand their roles.
03	Low-risk technical test Use a separate test environment or nominal-value setup. Never improvise with primary assets.
04	Record gaps Write down ambiguity, unavailable dependencies, conflicting instructions, and single points of failure.
05	Close and recheck Update the plan, then repeat the walkthrough until the sequence is clear.

Rehearsal date ______________________

Participants ______________________

Largest gap found ______________________

Next review date ______________________

Common failure modes

Use this list as a pre-mortem. Ask what would fail if the plan were needed today.

Only the seed exists	Nobody knows the asset map, dependencies, legal authority, or safe sequence.	☐ Addressed
Everything is together	One discovery, theft, fire, or coercion event compromises the whole plan.	☐ Addressed
The instructions are obsolete	Devices, software, people, and legal documents changed without a review.	☐ Addressed
One expert holds all context	The plan stops working if that person is unavailable or conflicted.	☐ Addressed
Family acts under pressure	An unsolicited helper, fake support account, or rushed transaction creates loss.	☐ Addressed
The plan was never tested	A small ambiguity becomes a major failure during a stressful event.	☐ Addressed

A legitimate helper does not need your seed phrase in a website, chat, email, or phone call. Treat urgency and unsolicited recovery help as warning signs.

Coordinate the legal and tax layer

Technical access does not automatically create legal authority. The people who can reach an asset and the people authorized to administer it may not be the same.

- ☐ Ask an estate-planning attorney how digital assets should be addressed in your jurisdiction.
- ☐ Confirm who has authority during incapacity, not only after death.
- ☐ Discuss privacy: public documents should not reveal wallet-specific information.
- ☐ Ask a tax professional what records beneficiaries and the estate may need.
- ☐ Document how records can be found without listing balances or addresses here.
- ☐ Review beneficiary intent after marriage, divorce, birth, death, relocation, or entity changes.

Questions for your professionals

How should digital assets be described	
Who receives authority and when	
What records should be preserved	
What privacy risks should be avoided	
What event should trigger an update	

Your annual review

Set a recurring date and review after any meaningful change. Do not use this review to expose or consolidate secrets.

- ☐ Inventory still matches the systems actually used.
- ☐ Trusted people, professionals, and backups remain appropriate.
- ☐ Instructions reference current devices and official software sources.
- ☐ Recovery materials remain intact under the chosen storage controls.
- ☐ No document accidentally contains wallet secrets or unnecessary financial detail.
- ☐ Legal documents and beneficiary intent remain aligned.
- ☐ The communication sequence is clear to someone other than the owner.
- ☐ A safe rehearsal has occurred since the last major change.

Review completed	
Next scheduled review	
Reviewed with	
Documents updated	
Rehearsal completed	

The safest plan is not the one with the most detail. It is the one that gives authorized people a clear, tested process while keeping access material protected.

Your next three actions

Choose specific actions you can complete without exposing wallet information.

ACTION 1

What I will do

Who is involved

Target date

ACTION 2

What I will do

Who is involved

Target date

ACTION 3

What I will do

Who is involved

Target date

Notes

Sources and responsible use

This workbook intentionally avoids prescribing a universal custody or succession architecture. Your legal jurisdiction, assets, family structure, threat model, and wallet technology determine what is appropriate.

Primary references

Bitcoin Improvement Proposal 39 describes mnemonic codes used to derive deterministic wallet seeds and lists the standard 12, 15, 18, 21, and 24-word lengths. https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki

The U.S. Internal Revenue Service explains that digital assets may have tax-reporting consequences and provides current digital-asset guidance. https://www.irs.gov/filing/digital-assets

The U.S. Federal Trade Commission warns consumers about cryptocurrency scams and unsolicited demands involving cryptocurrency. https://consumer.ftc.gov/scams

DIGITAL ASSET LEGACY WILL NEVER ASK FOR YOUR RECOVERY PHRASE, PRIVATE KEYS, WALLET ADDRESS, BALANCE, DEVICE SERIAL NUMBER, OR STORAGE LOCATION.

Version 1.0 | Prepared September 2026

For educational use. Review with qualified legal, tax, and security professionals before relying on any plan.