CUSTODY DUE-DILIGENCE CHECKLIST

SHEPLEY CAPITAL

Custody Due Diligence Checklist

Before you trust any platform with your crypto, run through this checklist

Before depositing funds into any exchange, wallet provider, custodian, or DeFi protocol... every item on this checklist should be verified. A single missed item has been the cause of catastrophic losses for individual investors. This checklist is designed to be completed fresh for every new platform.

A. CENTRALISED EXCHANGE (CEX) DUE DILIGENCE

Complete every item before depositing funds into a centralised exchange for the first time.

Regulatory & Legal Standing

- [ ] Exchange holds a valid Australian Digital Asset Services licence (or equivalent in its home jurisdiction)
- [ ] Exchange is registered with AUSTRAC as a Digital Currency Exchange provider (for Australian platforms)
- [ ] No active regulatory action, enforcement, or investigation identified via ASIC or AUSTRAC searches
- [ ] Terms of service reviewed — understand withdrawal conditions, account termination clauses, and fee structures
- [ ] Clear corporate entity identified — registered business name, ABN or equivalent, physical headquarters

Security & Custody Practices

- [ ] Exchange publicly discloses cold storage percentage (reputable platforms store 95%+ of assets offline)
- [ ] Proof of Reserves (PoR) audit published by a recognised third-party auditor within the last 12 months
- [ ] Bug bounty programme in place — signals active engagement with external security researchers
- [ ] Insurance policy in place for hot wallet holdings or platform hack events
- [ ] Two-Factor Authentication (2FA) mandatory or strongly enforced for all user accounts
- [ ] Withdrawal address whitelisting feature available
- [ ] Anti-phishing code feature available (custom phrase in all platform emails)

Operational Track Record

- [ ] Exchange has been operating for a minimum of 3 years without a major security incident
- [ ] No history of frozen withdrawals, insolvency events, or customer fund misappropriation
- [ ] Withdrawal process tested with a small amount before depositing significant capital
- [ ] Customer support responsiveness verified — test a non-urgent query before depositing
- [ ] Liquidity verified — trading volume on major pairs is genuine (check CoinMarketCap, Kaiko for data)
- [ ] Not identified on community blacklists (check crypto forums, Reddit, Trustpilot for red flags)

B. HARDWARE WALLET & SELF-CUSTODY DUE DILIGENCE

Complete every item when setting up a new hardware wallet or self-custody wallet for the first time.

Device Authenticity

- [ ] Device purchased directly from the manufacturer's official website — never from third-party resellers or marketplace platforms
- [ ] Packaging sealed and intact on arrival — any sign of tampering is grounds for return without use
- [ ] Device firmware verified as genuine during setup using the manufacturer's authenticity check process
- [ ] Firmware updated to latest version from official source before any funds are transferred to the wallet
- [ ] Device manufacturer is a recognised, established provider (e.g., Ledger, Trezor, BitBox, Coldcard)

Seed Phrase Setup

- [ ] Seed phrase written down by hand on paper during initial setup — no digital copy created at any point
- [ ] Seed phrase stored in at least two physically separate, secure locations
- [ ] Seed phrase tested via wallet recovery process on a second device before transferring significant funds
- [ ] Seed phrase never entered into any website, software, or online form
- [ ] No photographs taken of the seed phrase at any stage
- [ ] Metal backup solution considered for long-term storage (fire and water resistant)

- Ongoing Wallet Security

- [ ] PIN code set on hardware device — minimum 6 digits; not a date of birth or obvious number
- [ ] Passphrase (25th word) considered for additional security layer on high-value wallets
- [ ] Wallet addresses verified on the device screen before every transaction — never trust software display alone
- [ ] Small test transaction sent and received before moving large amounts to a new wallet
- [ ] DeFi connections reviewed and revoked regularly using a revocation tool (e.g., Revoke.cash)

C. DeFi PROTOCOL DUE DILIGENCE

Complete before connecting your wallet to or depositing funds into any DeFi protocol.

- [ ] Smart contract audited by a recognised security firm (e.g., Certik, Trail of Bits, OpenZeppelin) — audit report publicly available
- [ ] Development team publicly identified and verifiable — anonymous teams carry significantly higher rug pull risk
- [ ] Protocol has been operating for a minimum of 6 months without an exploit or emergency withdrawal event
- [ ] Total Value Locked (TVL) is genuine — verified via DeFiLlama or equivalent; not artificially inflated by protocol incentives
- [ ] Token economics reviewed — understand emission schedules, vesting, and who holds large token allocations
- [ ] Yield rate is sustainable relative to protocol revenue — unsustainable APY is a red flag for Ponzi mechanics
- [ ] Impermanent loss understood and modelled for any liquidity provision activity
- [ ] Connected wallet uses a separate warm wallet — hardware wallet should never be directly connected to DeFi
- [ ] Maximum approval amounts set to exact transaction amounts — avoid unlimited token approvals
- [ ] Exit liquidity exists — confirm you can withdraw your position in normal and stressed market conditions

D. PERSONAL ACCOUNT SECURITY CHECKLIST

Review these items across all platforms and devices you use for crypto activity.

- [ ] Authenticator app 2FA enabled on every exchange and crypto-related account — no SMS 2FA
- [ ] Unique, strong password used for every exchange — stored in a reputable offline or local password manager
- [ ] Dedicated email address used exclusively for crypto accounts — secured with strong password and authenticator 2FA
- [ ] Withdrawal address whitelisting enabled with a time-delay on all major exchanges
- [ ] Anti-phishing code set on all exchanges that support the feature
- [ ] No crypto activity conducted on public Wi-Fi without a VPN
- [ ] Devices used for crypto activity have up-to-date antivirus and operating system security patches
- [ ] No crypto browser extensions installed other than verified wallet extensions (MetaMask, etc.)
- [ ] Exchange bookmarks used — never navigate to exchanges via search results or email links
- [ ] Friends, family, and social connections are not informed of specific portfolio value or holdings
- [ ] Estate plan in place — trusted person has access to wallet recovery information in case of incapacitation

GENERAL ADVICE DISCLAIMER

This checklist is produced by Shepley Capital (shepleycapital.com) for general educational purposes only. It does not constitute financial advice, security advice, or any other form of regulated advice. No checklist can guarantee the security of your assets — the crypto landscape evolves rapidly and new risks emerge regularly.

Completing this checklist reduces but does not eliminate risk. Always conduct your own additional research specific to each platform and your individual circumstances.