Sicherheitsleitlinien im Umgang mit Software- und Hardwarewallets

Stand: 13.11.2025

Diese Leitlinien nennen bestimmte Mindeststandards im Umgang mit Software- und Hardwarewallets und sind nicht abschließend. Sie ersetzen keine individuelle Sicherheitsberatung und begründen keine Haftung des Anbieters für Handlungen oder Unterlassungen des Kunden.

1. Allgemeine Mindeststandards für Software- und Hardwarewallets

Originalquellen & Integrität: Download/Erwerb ausschließlich von offiziellen/autorisierten Quellen; Prüfsummen/Signaturen (sofern angeboten) verifizieren; keine „vorinitialisierten" Geräte annehmen.

Seed/Recovery-Phrase: jedenfalls bei Hardwarewalles im Idealfall nur offline erzeugen/anzeigen; keine Fotos/Scans/Cloud-Backups; mindestens 2 Backups (Papier/Metall) an getrennten sicheren Orten; keine Weitergabe an Dritte.

Passwörter/Passphrase: Starke, einzigartig verwendete Passwörter; BIP39-Passphrase nur bei vollem Verständnis der Risiken; getrennt vom Seed dokumentieren und aufbewahren.

Wiederherstellung testen: Recovery mit geringen Beträgen vorab proben; Notfallplan (Auffindbarkeit von Hinweisen, ohne Seeds zu offenbaren) erstellen.

Transaktionen & Adressen: Vor höheren Beträgen Testtransaktion; Adresswiederverwendung vermeiden; Coin-Control bewusst nutzen; xpubs sparsam teilen (Watch-Only nur bei vertrauenswürdigen Tools).

Betrugs-/Phishing-Schutz: URLs manuell/Lesezeichen; kein Klick auf Links aus Mails/Chats; „Support" fragt nie nach dem Seed; keine Fernwartung auf Systemen mit Wallets zulassen.

Updates: Wallet-Software/Firmware nur von Hersteller-Seiten beziehen; nach Updates Funktion mit kleinen Beträgen verifizieren.

Physische Sicherheit: Geräte/Backups gegen Diebstahl, Feuer, Wasser sichern (Tresor/Schließfach); geografisch getrennte Lagerung; Zugriff nur für einen minimalen Personenkreis.

2. Zusätzliche Anforderungen für Softwarewallets

Gehärtetes Endgerät: Aktuelles OS, Voll-Datenträgerverschlüsselung, aktueller Browser; kein Jailbreak/Root; separates Benutzerprofil für die Wallet empfohlen.

Cloud & Backups: Cloud-Backups der Wallet/seiner Dateien deaktivieren; regelmäßige Offline-Sicherungen nach Herstellerhinweis.

Angriffsfläche reduzieren: Wenige Browser-Erweiterungen; keine fraglichen „Security-Tools"; Clipboard-/Screenshot-Uploads vermeiden; Antivirus/Firewall aktuell.

Mobile Nutzung: Geräte-PIN/BIOMetrics, Auto-Sperre kurz; kein Entsperren auf fremden Netzen; keine Nutzung auf kompromittierten/leihweisen Geräten.

Watch-Only-Setups: Für Übersicht Watch-Only auf dem Hauptrechner, private Schlüssel auf separatem Gerät belassen.

3. Zusätzliche Anforderungen für Hardwarewallets

Beschaffung & Erstinbetriebnahme: Originalverpackt vom Hersteller/autorisiertem Händler; auf Manipulation achten; Erstinitialisierung selbst durchführen.

Seed-Erzeugung am Gerät: Seed ausschließlich am Hardware-(Display) generieren/anzeigen; niemals in Computer/Telefon eintippen.

Adress-/Transaktionsprüfung: Empfangs- und Wechseladressen sowie Transaktionsdetails auf dem Gerätedisplay prüfen und erst dann signieren.

Firmware-Sicherheit: Firmware-Updates nur von Hersteller-Seiten; ggf. Prüfsumme/Fingerprint prüfen; Update erst nach Backup durchführen.

Multisig & Redundanz: Für höhere Werte Multisig mit unterschiedlichen Herstellern/Standorten erwägen; Ersatzgerät/Recovery-Plan vorhalten und testen.

ENDE DER SICHERHEITSLEITLINIEN