Veilo Layer LLC — Risk Disclosure

Risk Disclosure

Effective Date: April 30, 2026 **Last Updated:** May 12, 2026

1. Read Before You Use Veilo

This Risk Disclosure is issued by **Veilo Layer LLC** ("**Company**", "**Veilo**"), a Wyoming limited liability company (Wyoming Secretary of State Entity ID **2026-001871701**, formed January 20, 2026), and is incorporated by reference into the Veilo Terms of Service. It describes risks inherent to using cryptocurrency, blockchain technology, zero-knowledge cryptography, and the specific architecture of the Veilo Protocol and the Services (each as defined in the Terms of Service).

By accessing or using the Services, you acknowledge, understand, and agree that your use of the Veilo Protocol and the Services involves significant technical, operational, legal, regulatory, and economic risks, and that all such use is undertaken **entirely at your own risk**. To the maximum extent permitted by applicable law, neither the Company, the Protocol, nor any other Veilo Party (as defined in the Terms of Service) shall be responsible or liable for any loss, damage, delay, inaccessibility, or inability to use the Services or any component thereof, except as expressly required by law that cannot be lawfully waived.

The Services are not offered to U.S. persons or to persons in any other Restricted Jurisdiction. See the Acceptable Use Policy, Section 2. By using the Services, you represent that you are not a Restricted Person.

By using Veilo you acknowledge that you have read, understood, and accepted these risks.

If you do not understand any of the risks below, **do not use the Services until you do.** Consider consulting a qualified financial, legal, or technical advisor licensed in your jurisdiction (other than the United States).

2. Cryptocurrency and Blockchain Risks

2.1 Volatility

The value of cryptocurrencies and tokens can fluctuate significantly, including to **zero**, in short periods. There is no guarantee that any token you hold or transact in will retain any particular value, retain liquidity, or remain tradeable.

2.2 Transaction finality

Once a transaction is confirmed on the Solana blockchain, it is **irreversible**. Veilo cannot reverse, cancel, or refund a confirmed transaction, even if it was sent to the wrong address, contained the wrong amount, or was the result of a mistake or compromise.

2.3 Network risk

The Solana blockchain may experience:

- **Outages** or degraded performance during which transactions cannot be submitted or confirmed
- **Forks** or contentious upgrades that change the protocol
- **Reorganisations** that retroactively change the order of confirmed transactions
- **Congestion** that increases fees or causes transactions to fail
- Discovery of **bugs** that affect consensus or transaction validity

These events are outside Veilo's control. Veilo is not liable for any loss caused by Solana network behaviour.

2.4 RPC provider dependency

Veilo relies on third-party Solana RPC providers (currently Helius). RPC outage or compromise can cause delayed, missed, or incorrect data display in the Service. Always treat balances and transaction status as **best-effort estimates** until confirmed via independent block explorer.

2.5 Fees

Solana network fees and DEX fees are paid to third parties and may change without notice. Estimated fees displayed in the Service may differ from actual fees charged.

3. Smart-Contract and Cryptographic Risks

3.1 Smart-contract risk

The Veilo Privacy Pool program (`privacy-program`) is a Solana smart contract. Smart contracts:

- May contain **bugs**, despite careful development and audit (most recent audit: March 2026, identifying 1 medium-severity finding)
- May behave **unexpectedly** under conditions not anticipated by the developers
- May be **exploited** by adversaries who discover vulnerabilities before they are patched
- Are **immutable** in their deployed form — bugs may not be patchable without redeploying and migrating users
- May depend on other smart contracts (e.g., Jupiter, Raydium, the SPL Token program) that are themselves subject to the same risks

A smart-contract bug may result in **partial or total loss** of funds in the Privacy Pool.

3.2 ZK-SNARK / cryptographic risk

The Veilo Privacy Pool uses **Groth16 zero-knowledge proofs over the BN254 elliptic curve**, with **Poseidon** as the hash function. The cryptographic primitives are widely used and considered secure under current assumptions. However:

- A **mathematical breakthrough** could weaken or break the cryptography (e.g., advances in elliptic-curve cryptanalysis, factoring, or ZK-SNARK soundness)
- A **trusted setup** is required for Groth16 — if the setup ceremony was compromised, an attacker may be able to forge proofs and mint Privacy Pool funds out of thin air. Veilo uses `Powers of Tau ceremony` . Users rely on the integrity of that public ceremony.
- A **circuit bug** could allow invalid proofs to verify on-chain, leading to fund loss
- A **prover bug** could fail to produce valid proofs, locking funds

A cryptographic break or a circuit bug may result in **partial or total loss** of funds in the Privacy Pool, or in **failure of privacy guarantees**.

3.3 Quantum-computing risk

The cryptography underlying the Solana blockchain (Ed25519 signatures) and the Veilo Privacy Pool (BN254 pairings) is **not quantum-resistant**. A sufficiently large quantum computer in the future could break these primitives, potentially compromising both the security of funds and the privacy of past transactions.

4. Privacy Risks

4.1 Privacy is probabilistic

The Privacy Pool reduces the on-chain link between sender and recipient, but **does not provide unconditional anonymity**. Your privacy depends on:

- The **size of the anonymity set** (the number of other users in the Pool whose actions are indistinguishable from yours)
- The **timing patterns** of your deposits, transfers, and withdrawals
- The **amounts** you transact (round-number amounts and round trips can be correlated)
- Your behaviour **outside** the Pool (linking your “shielded” address to a “transparent” identity defeats the privacy)

Even with optimal use, certain statistical attacks may degrade privacy below the size of the nominal anonymity set.

4.2 Relayer compromise

Private withdrawals, transfers, and swaps are submitted by a Relayer (whether the Reference Relayer operated by the Company, an independent third-party Relayer, or a Relayer you operate yourself), which receives your fully signed transaction, generates the broadcast payload, and submits it to Solana. While Relayers are designed to minimise the data they can observe:

- A Relayer may **temporarily process** transaction payloads to construct the broadcast envelope;
- A Relayer **knows the IP address** from which a request originated;
- A Relayer **observes timing**;
- A compromised, coerced, or maliciously-operated Relayer (whether the Reference Relayer or an independent Relayer) could correlate request payloads with on-chain outputs and compromise privacy.

The Company designs the Reference Relayer’s architecture to limit its exposure and audits its infrastructure, but **the Company cannot guarantee that any Relayer (including the Reference Relayer) will never be compromised, censored, coerced, or compelled by lawful process**. Relayers other than the Reference Relayer operate independently and are outside the Company’s control; the Company makes no representation or warranty about their security, availability, or conduct.

4.3 Side-channel and metadata risk

Privacy may be compromised by:

- **IP metadata** captured by Veilo or third parties (we record IP for security and abuse prevention; see Privacy Policy)
- **Network observers** between you and Veilo (always use Tor or a VPN if your threat model warrants)
- **Device compromise** (malware, screen-recording, keylogger)
- **Voluntary disclosure** to others
- Linking via **deposit address ↔ withdrawal address** if you reuse addresses
- Linking via **off-chain identifiers** (KYC at exchanges, social media disclosure)

4.4 Forensic and chain-analysis improvements

Blockchain forensic firms continually improve their ability to deanonymise pool-based privacy systems. Privacy that is sufficient today may be insufficient in the future. **You should not rely on Veilo for privacy guarantees that depend on multi-year secrecy.**

4.5 No protection against legal compulsion

Privacy from technical observation does not provide protection from legal compulsion. If you are subject to a court order to disclose your transaction history, the Veilo Service does not relieve you of that obligation. **Veilo is not a tool for evading legal obligations.**

---

5. Self-Custody Risks

5.1 Recovery-phrase loss

Your **12-word BIP-39 recovery phrase** is the single key to your self-custody wallet. **If you lose it, your funds are permanently inaccessible.** Veilo cannot recover it. No other party can recover it.

- Write it down on paper or metal
- Store it in a secure location (or multiple)
- Do not photograph it
- Do not store it in cloud storage
- Do not share it with anyone, ever — Veilo will never ask for it

5.2 Recovery-phrase theft

Anyone who obtains your recovery phrase has **full control** of your wallet. Phishing, malware, social engineering, and physical theft are all real threats.

5.3 Password loss

Your password locks the encrypted recovery phrase on your device. If you forget the password, you must restore your wallet from the recovery phrase. **If you have also lost the recovery phrase, your funds are permanently inaccessible.**

5.4 Device compromise

If your device is compromised by malware while your wallet is unlocked, an attacker can sign transactions or steal your password. Veilo's encryption protects against device theft when the wallet is locked, but not against malware running while the wallet is in use.

5.5 Approving transactions

You are responsible for **reviewing every transaction** before approving it. Adversarial dApps and websites can craft transactions that appear benign but actually transfer your funds, grant unlimited token approvals, or otherwise harm you. Veilo displays the transaction details to you, but cannot evaluate the intent or safety of every counterparty.

---

6. Privacy-Pool Specific Risks

6.1 Note loss

Your encrypted **Notes** are the only proof of ownership of funds in the Privacy Pool. If your Notes are lost and cannot be recovered:

- Funds remain in the Privacy Pool but **may be permanently inaccessible**
- Veilo **cannot help recover** Notes whose contents we do not have the keys to decrypt

To minimise Note-loss risk: - Sign in to your wallet at least once after each deposit so the encrypted backup is synced - Do **not** uninstall the wallet while you have funds in the Pool — withdraw first - Maintain access to your recovery phrase and password (which decrypt the Notes)

6.2 Relayer unavailability

A Relayer is required to broadcast private withdrawals, transfers, and swaps to Solana. If no compatible Relayer is available to you, you cannot perform these operations until a Relayer becomes available.

If the Company-operated **Reference Relayer is permanently shut down** for any reason (regulatory action, business cessation, security incident, court order, etc.), the on-chain Privacy Pool will continue to exist, and:

- You retain your Encrypted Notes;
- You may use any **compatible third-party Relayer** (if one exists) or **operate your own Relayer** (if you have the technical means) to access your value;
- The Company may publish documentation to facilitate self-relay or third-party-relayer operation, but is **not contractually obligated** to do so.

There is no guarantee that any alternative Relayer will exist at any given time, that self-relay will be technically feasible for non-technical Users, or that you will be able to access value within the Privacy Pool following Reference Relayer shutdown. **Value held within the Pool may become difficult or impossible to access in the event of permanent Reference Relayer shutdown.**

A Relayer's inability or refusal to submit a transaction does **not** constitute freezing, seizure, or custody of your value — ownership of value within the Privacy Pool remains with you at all times, evidenced by your Encrypted Notes. However, execution dependence on Relayer availability means that effective access may be temporarily or permanently impaired.

6.3 Anonymity-set decay

If usage of the Privacy Pool declines, the anonymity set shrinks and privacy guarantees weaken. The privacy you experience today is not guaranteed in the future.

6.4 Migration / contract upgrades

If a successor version of the Veilo Privacy Pool is deployed, Users may be expected to migrate value from the old Pool to the new Pool. The original Pool may eventually become unmaintained, with reduced anonymity-set growth, potentially limited Relayer access, and degraded privacy.

6.5 Concentrated Relayer risk

At launch the Company operates the **Reference Relayer**, which may, in practice, be the only or principal Relayer available to Users. This creates concentration risk: a single point of failure for Service availability and a single point of trust for privacy assumptions. The Veilo Protocol is permissionless and other parties may operate compatible Relayers, but as of the Effective Date no such third-party Relayers are known to be in production operation. The Company is not contractually obligated to maintain the Reference Relayer or to ensure that a successor or alternative Relayer is available.

---

7. Regulatory and Legal Risks

7.1 Evolving regulation

Cryptocurrency regulation varies widely by jurisdiction and is **rapidly evolving**. Laws may be enacted, modified, or interpreted in ways that:

- Restrict or prohibit your use of the Service
- Require Veilo to register with authorities (FinCEN MSB, MiCA CASP, BitLicense, etc.)
- Require Veilo to implement KYC, transaction monitoring, or transaction blocking
- Result in the Service being **unavailable** in your jurisdiction
- Create personal legal liability for you if your use is determined to be unlawful

You are solely responsible for understanding and complying with all laws applicable to your use of the Service in your jurisdiction.

7.2 Sanctions risk

The use of privacy tools in the cryptocurrency context has been the subject of sanctions enforcement, including the OFAC sanctions of Tornado Cash in 2022 (lifted in 2025). Although the regulatory environment has shifted to recognise legitimate privacy uses (see U.S. Treasury report to Congress, March 2026), the legal status of pool-based privacy is **not settled** and may be challenged in the future.

You agree that you will not use Veilo to evade sanctions, and Veilo will cooperate with sanctions authorities as required by law. See our Compliance Statement.

7.3 Tax obligations

Crypto transactions are taxable events in most jurisdictions. Deposits, withdrawals, transfers, and swaps may give rise to tax obligations (capital gains, ordinary income, VAT, etc.). Privacy features do **not** reduce or eliminate tax obligations. **You are solely responsible for tracking and reporting your transactions for tax purposes.**

Veilo does not provide tax forms (e.g., 1099, P2P), and Veilo does not provide tax advice. Consider using a crypto tax service or consulting a qualified tax advisor.

7.4 Securities and other financial regulation

Some tokens may be considered **securities** in certain jurisdictions. Trading in unregistered securities may be unlawful. Veilo does not assess whether any specific token is a security. **You are responsible for the legal status of every token you transact.**

7.5 No deposit insurance

Value held in the Privacy Pool, in your self-custody wallet, or in any cryptocurrency form is **not insured** by the FDIC, the SIPC, the FSCS, or any other government deposit-insurance scheme.

7.6 Compelled disclosure and enforcement risks

Enforcement authorities may seek to compel you (or the Company, or any independent Relayer or other Protocol participant) to disclose identifiers, viewing keys, master viewing keys, decryption keys, transaction metadata, or transactional records. Failure to comply may result in personal civil or criminal liability. **The Services do not relieve you of any legal obligation to make truthful disclosure under applicable law.** Veilo is not a tool for evading legal obligations, court orders, tax reporting, sanctions compliance, or law-enforcement requests directed at you.

You may incur registration, licensing, disclosure, reporting, tax, or AML/KYC obligations under the laws of your jurisdiction, including obligations relating to selective disclosure using viewing keys or master viewing keys. Privacy-enhancing transactions may attract enhanced regulatory or law-enforcement scrutiny.

Users operating their own Relayer infrastructure may incur separate licensing, AML, sanctions, or reporting obligations arising from fee abstraction or broadcast services. The Company makes no representation about the regulatory status of independent Relayer operation in any jurisdiction.

Encrypted balances may complicate future inheritance, insolvency resolution, civil litigation, audits, divorce, bankruptcy, tax investigations, or claims to ownership. Conflicts of law among jurisdictions may affect validity, enforceability, or legal recognition of cryptographic transfers, ownership proofs, or finality.

7.7 Counterparty taint risk

You may interact unknowingly with addresses associated with tainted, illicit, or sanctioned funds, potentially exposing yourself to seizure, forfeiture, freezing, regulatory inquiry, or enforcement action. The Company's screening operates only on the on-chain participants observed at the time of submission and cannot identify all counterparties whose history may, in retrospect, be deemed tainted. **You are solely responsible for any consequences arising from counterparty taint.**

7.8 Restricted-Person and jurisdictional access risk

The Services are not offered to U.S. persons or to persons in other Restricted Jurisdictions (see the Acceptable Use Policy). If you are a Restricted Person and you nevertheless access the Services in violation of the Terms of Service:

- you are in material breach of the Terms of Service;
- the Company may refuse Service, suspend or terminate your account, refund or withhold fees in its discretion, and report the activity where required;

- you may have no remedy against the Company in respect of any loss, delay, or unavailability you experience;
- you may have personal civil or criminal liability under the laws applicable to you, including securities laws, anti-money-laundering laws, money-transmission laws, and consumer-protection laws of any jurisdiction in which you are located;
- you indemnify the Veilo Parties on the terms of Section 18 of the Terms of Service for the entirety of such use.

---

8. Third-Party Risks

8.1 Jupiter and DEX integrations

Private Swaps route through Jupiter, Raydium CPMM/AMM, and OpenBook (Serum). These third-party protocols are subject to their own bugs, exploits, and outages. A failed swap may result in funds being stuck temporarily; in extreme cases, a DEX exploit could result in fund loss.

8.2 Price oracle risk

Token prices displayed in the Services come from third-party providers (CoinGecko, DexScreener, GeckoTerminal). Prices may be inaccurate, delayed, or manipulated. **Do not rely on displayed prices for trading decisions on a leveraged or time-sensitive basis.**

8.3 App-store risk

The Mobile App is distributed via Apple App Store, Google Play, and as a sideloaded `.apk`. Apple or Google may suspend or remove the app from their stores at any time, for any reason, with or without notice. The browser extension is distributed via the Chrome Web Store, subject to the same risk.

8.4 Hosting provider risk

The Company's off-chain infrastructure is hosted on third-party providers (Vercel, Cloudflare, MongoDB Atlas, and others). Provider outages, terminations, data breaches, account suspensions, or refusals of service may affect the availability and security of the off-chain components of the Services. The Company does not control, and is not responsible for, the conduct, availability, or security of its hosting providers.

8.5 Independent Relayer risk

The Veilo Protocol is permissionless and any party may operate a Relayer. Independent Relayers operated by third parties or by Users themselves are **not** agents, custodians, fiduciaries, or service providers of the Company. The Company does not control, audit, or monitor independent Relayers and makes no representation or warranty about their security, availability, reliability, fee level, sanctions screening, AML/CFT controls, or compliance posture. If you select an independent Relayer to broadcast your transaction, you do so entirely at your own risk and subject to the Relayer's own terms and conduct.

8.6 Interface, frontend, and dependency risk

Users may rely on Company-operated interfaces, dashboards, SDKs, APIs, or reference implementations to interact with the Veilo Protocol. Such interfaces may contain bugs, inaccuracies, latency, stale data, misconfigurations, or display errors that do not reflect actual on-chain state. Interface availability, correctness, or usability may be affected by software defects, upgrades, browser compatibility, mobile-operating-system changes, third-party dependencies, hosting outages, app-store removal, or network disruption.

The authoritative record of ownership, balances, and execution is the Solana blockchain itself. The Company does not guarantee that any interface accurately reflects Protocol state at any given time. Users are encouraged to independently verify balances, transactions, and Protocol state using a Solana block explorer or by running their own indexer.

8.7 Data-integrity and indexing risk

The Services may rely on indexers and off-chain data-aggregation systems to present balances, transaction history, fee estimates, or Protocol state. Such systems may be incomplete, inaccurate, delayed, censored, or unavailable. Incorrect or missing indexed data may cause Users to make incorrect assumptions regarding balances, execution status, or eligibility, **for which the Company bears no responsibility**.

8.8 Force majeure and external intervention

Access to or operation of the Services may be disrupted or permanently impaired by events beyond the Company's reasonable control, including government action, regulatory intervention, sanctions, court orders, infrastructure seizure, internet outages, cloud-service termination, app-store removal, force majeure events, geopolitical events, or pandemics. Such events may result in loss of access, inability to transact, or permanent inaccessibility of value, without liability to the Veilo Parties.

---

9. Operational Risks

9.1 Software bugs in the wallet

Despite testing, the wallet software (Extension, Mobile App, web dApp) may contain bugs that:

- Display incorrect balances or transaction status
- Fail to send or receive transactions
- Lock funds in error states
- Cause partial loss of Notes

We will fix bugs as they are discovered, but cannot guarantee the wallet is bug-free.

9.2 Phishing

Adversaries may distribute fake versions of the Veilo Wallet, the Site, or the dApp, attempting to capture your recovery phrase or password. Always:

- Verify URLs (`https://veilo.network` , `https://docs.veilo.network`)
- Install the Extension only from the official Chrome Web Store listing
- Install the Mobile App only from the official Apple App Store, Google Play, or `https://veilo.network/download`
- Verify cryptographic signatures of the `.apk` if sideloading
- Never enter your recovery phrase into any website, app, or form other than the official Veilo Wallet's restore flow

9.3 Service discontinuation

The Company may discontinue any of the Services at any time, for any reason, with or without notice. While the on-chain Privacy Pool Smart Contracts will continue to exist independent of the Company, off-chain Services (Reference Relayer, Mobile App back end, encrypted-Note-backup service, web dApp, Site, Docs) may become unavailable. Plan accordingly.

9.4 No retention or rollback of cryptographic state

Protocol-level state transitions and cryptographic commitments are enforced through zero-knowledge proofs. Invalid commitments cannot be submitted to the Protocol, as commitment correctness is enforced within the ZK-proof constraints, but cryptographic state once committed is final. Once a deposit, claim, transfer, or swap is confirmed on Solana, it is final, irrevocable, and irreversible. No Veilo Party can reverse, unwind, or recover transferred assets.

10. No Duty, No Guarantee, No Recourse

10.1. **No duty.** The Veilo Protocol is experimental, decentralized, permissionless, and provided on a non-custodial basis. No Veilo Party owes you any duty of care, fiduciary obligation, custodial duty, operational responsibility, agency obligation, or guarantee in respect of: execution, settlement, confidentiality, anonymity, recoverability, continued availability of the Protocol or any associated infrastructure, the conduct or solvency of any Relayer (whether the Reference Relayer or independent), the conduct of any validator, RPC provider, MPC node operator (if and when adopted), or other Protocol participant.

10.2. **No guarantee.** No Veilo Party guarantees:

- execution of any transaction;
- continued availability of the Services or the Protocol;
- liveness of the Reference Relayer or of any independent Relayer;
- balance confidentiality, transaction privacy, anonymity, untraceability, or unlinkability;
- solvency, security, or correct functioning of the Protocol, any Smart Contract, any Relayer, any third-party service, or any other component of the system;
- the absence of bugs, vulnerabilities, exploits, attacks, censorship, or compromise;
- the value, liquidity, or legal status of any supported token;
- the availability or accuracy of indexed data, price data, or any other displayed information;
- the regulatory status of the Services or your transactions in any jurisdiction.

10.3. **No recourse.** No Veilo Party has any obligation to:

- refund, reimburse, replace, restore access to, retrieve, or compensate for any loss, delay, error, failure, unavailability, or compromise of the Protocol, the Services, or any value;
- operate, maintain, replace, subsidize, expedite, or restore any Relayer (including the Reference Relayer);
- recover lost recovery phrases, passwords, viewing keys, master viewing keys, decryption keys, or Encrypted Notes;
- decrypt encrypted Note backups or any other encrypted material;
- modify, freeze, seize, blacklist, or otherwise alter on-chain state;
- pursue remediation, indemnification, or restoration on behalf of any User; or
- compel any third party (independent Relayer, validator, MPC node operator, RPC provider, wallet provider, indexer) to take any action.

10.4. **You may have no remedy.** You expressly acknowledge and agree that, to the maximum extent permitted by applicable law, you may have **no legal or equitable remedy against any Veilo Party** in respect of any loss, delay, unavailability, compromise, or failure of any component of the Protocol or the

Services. The allocation of risk under these Terms is fundamental to the Company's decision to provide the Services. See Sections 17 (Disclaimer), 18 (Indemnification), and 19 (Limitation of Liability) of the Terms of Service.

---

11. Acknowledgement

By accessing or using the Services, you acknowledge, understand, and agree that:

- you have read and understood this Risk Disclosure;
- you accept all of the risks described herein;
- you understand that the list of risks above is **not exhaustive** and that other risks not foreseeable today may arise;
- you will not use the Services if your tolerance for these risks is low;
- you will not invest more value than you can afford to lose;
- no Veilo Party is your fiduciary, financial advisor, broker, investment manager, or money services business;
- you are not a Restricted Person (including not a U.S. person);
- you are solely responsible for understanding and complying with all laws applicable to you in your jurisdiction.

If at any time you no longer accept these risks, immediately stop using the Services and (if applicable) withdraw any value held within the Privacy Pool.

---

12. Contact

Questions about risks: `legal@veilo.network` or `support@veilo.network`.

Built with zero-knowledge proofs on Solana.