Ciforus AML Policy

Risk-based anti-money laundering and sanctions control policy

Brand	Ciforus
Series	Legal and trust documentation
Prepared	April 2026
Status	Launch-ready draft with counsel review

This document reflects the current Ciforus product, token, privacy, and launch narrative and will be updated with the project progress.

Effective Date: April 4, 2026

Document Status: Policy for launch preparation

Applies To: token onboarding, presale participation, wallet-linked payment features, and higher-risk financial or compliance-sensitive activity connected to the Ciforus ecosystem

Important Notice

This Anti-Money Laundering Policy explains the risk-based approach Ciforus may use to reduce money-laundering, terrorist-financing, sanctions, fraud, and other illicit-finance risks in connection with the CIFORUS token ecosystem and related financial or wallet-linked activity.

Ciforus is not trying to behave like a retail bank. However, where token sales, wallet-linked payment flows, or compliance-sensitive activity are involved, Ciforus may need to apply onboarding, screening, recordkeeping, review, or refusal controls.

This document is a launch-stage draft informed by risk-based AML principles, including FATF guidance for virtual assets and virtual asset service providers. It should be reviewed by qualified legal and compliance counsel before final publication.

1. Purpose

The purpose of this policy is to:

- support lawful and responsible operation of token-related and payment-related services
- reduce the risk that Ciforus infrastructure is used for money laundering, sanctions evasion, fraud, terrorist financing, or other prohibited conduct
- preserve the integrity of the Ciforus ecosystem, including the CIFORUS token
- explain the controls Ciforus may apply before or during token participation or higher-risk financial activity

2. Scope

This policy may apply to:

- token presale participation
- token purchase requests
- wallet-linked subscription or payment flows
- large, unusual, or higher-risk transactions
- wallet verification where financial risk controls are needed

- users, purchasers, counterparties, or business partners involved in higher-risk financial activity connected to Ciforus

Ciforus may apply this policy selectively based on risk, service type, jurisdiction, transaction profile, product phase, and legal requirements.

3. Risk-Based Approach

Ciforus follows a risk-based approach. That means Ciforus may apply stronger checks where risk is higher and lighter checks where risk is lower.

Risk may be assessed using factors such as:

- jurisdiction
- sanctions exposure
- wallet behavior
- transaction size
- transaction pattern
- source-of-funds concerns
- use of mixers, obfuscation tools, or other red-flag behaviors
- politically exposed person or adverse-media risk
- unusual onboarding or identity inconsistencies

Ciforus is not required to publish all internal risk thresholds, screening logic, or review triggers.

4. Eligibility and Restricted Users

Ciforus may refuse, block, or restrict access where a person or transaction appears to involve:

- a sanctioned person or entity
- a sanctioned, embargoed, or prohibited jurisdiction
- a person acting on behalf of a sanctioned or prohibited party
- false, misleading, or incomplete compliance information
- suspicious, abusive, or clearly unlawful activity
- source-of-funds concerns that are not reasonably resolved

Ciforus may also limit or deny participation where doing so is prudent for legal, regulatory, reputational, or operational reasons.

5. Customer Due Diligence

Where appropriate, Ciforus may require one or more of the following before allowing or continuing token-related participation:

- confirmation of identity
- proof of control over a wallet
- residency or jurisdiction information
- sanctions screening
- source-of-funds or source-of-wealth explanation
- enhanced due diligence for higher-risk users or transactions
- declarations regarding beneficial ownership or control

Failure to provide requested information may result in delay, refusal, suspension, or cancellation of access.

6. Ongoing Monitoring and Review

Ciforus may review transactions, wallet activity, and user behavior on an ongoing or event-driven basis. Review may occur before, during, or after a transaction, onboarding event, or entitlement request.

Ciforus may monitor for:

- inconsistent or suspicious transaction patterns
- high-risk wallet interactions
- sanctions-related indicators
- structuring or evasion behavior
- fraudulent or deceptive conduct
- patterns inconsistent with the stated purpose of participation

7. Source of Funds and Wallet Integrity

Ciforus may request information or supporting material reasonably designed to confirm that funds used for token-related activity are lawful and under the control of the participant.

Where risk is elevated, Ciforus may refuse participation involving:

- wallets linked to illicit-finance indicators
- funds believed to be proceeds of crime or fraud
- unexplained or implausible source-of-funds information

- attempts to obscure ownership or origin without a legitimate explanation

8. Transaction Refusal, Suspension, and Freezing

Ciforus may decline, hold, suspend, or cancel a transaction, onboarding request, wallet link, or token-related entitlement if:

- AML or sanctions review is not satisfied
- legal risk is unresolved
- a technical or security concern exists
- a regulator, court, or legal process requires action
- the transaction appears suspicious, abusive, or unlawful

Ciforus may preserve records or cooperate with competent authorities where legally required.

9. Finality and Refund Position

Completed token purchases are **final and non-refundable**, except where non-waivable mandatory law requires otherwise.

That said:

- a pending transaction may be delayed or not processed while AML, sanctions, or security review is ongoing
- Ciforus may refuse to complete a transaction if eligibility or compliance requirements are not met
- where funds are held, blocked, or returned, the process may depend on legal constraints, technical feasibility, and the specific transaction state

Nothing in this policy obligates Ciforus to complete, settle, or honor a transaction that it reasonably believes should not proceed.

10. Recordkeeping

Ciforus may keep records related to compliance, token participation, and risk review for as long as reasonably necessary to:

- meet legal or regulatory obligations
- preserve evidence of screening or decision-making
- investigate suspicious activity
- resolve disputes or audits
- protect the integrity of the service

11. Reporting and Cooperation

Where required by applicable law, Ciforus may report suspicious activity, respond to lawful requests, or cooperate with competent authorities, regulators, courts, and enforcement bodies.

Ciforus is not required to notify a user if doing so would be unlawful, inappropriate, or contrary to the integrity of an investigation.

12. Privacy and Data Handling in AML Processes

Ciforus remains a privacy-first platform. Even so, AML-related review may require collection or verification of readable compliance information in specific cases.

Ciforus will aim to:

- collect only information reasonably necessary for risk review
- protect compliance records with appropriate security controls
- separate higher-risk compliance handling from ordinary user-facing product experience where practical
- avoid unnecessary disclosure of sensitive information

At the same time, users should understand that compliance records, identity materials, and transaction-review files are not the same as end-to-end encrypted private content. If Ciforus receives readable compliance information, that information may be retained, reviewed, and disclosed where legally required.

13. No Evasion, Circumvention, or Structuring

Users may not attempt to evade this policy by:

- splitting activity to avoid review thresholds
- using false identities or borrowed credentials
- masking beneficial ownership
- routing activity through third parties to conceal the true participant
- using wallets or services primarily to hide illicit origin or sanctions exposure

14. Policy Updates

Ciforus may revise this AML Policy at any time to reflect legal developments, product changes, token-launch needs, or improved compliance controls.

15. Contact

Compliance inquiries and lawful legal notices relating to this policy may be directed through the official Ciforus legal or compliance contact channels published on the Ciforus website.

16. Final Note

This AML Policy is intended to balance two things that matter to Ciforus: strong privacy by design and responsible financial-risk control where token or payment activity creates higher legal exposure.