Risk Disclosure Statement

Principal risks associated with ZEND and the Trnznd platform

Issuer	Trnznd SA, a sociedad anonima incorporated under the laws of the Republic of Panama
Digital Asset	ZEND
Document Type	Risk Disclosure Statement
Version	1.0
Effective Date	29th June 2026
Website	www.trnznd.io

Important Notice

This Risk Disclosure Statement is provided to help users understand the principal risks associated with accessing the Trnznd platform, acquiring, holding, transferring, using, minting, or redeeming ZEND.

ZEND is not legal tender, is not government-backed, is not a bank deposit, is not insured by any deposit protection scheme, and does not represent equity, debt, ownership rights, governance rights, dividend rights, or profit participation rights in Trnznd or any affiliate.

This document does not constitute legal, financial, investment, tax, accounting, regulatory, fiduciary, or other professional advice. Users remain solely responsible for independently assessing whether ZEND is appropriate, lawful, and suitable for their own purposes.

1. Nature of ZEND

ZEND is designed as a multi-currency digital settlement token for use in payments, settlement activity, treasury movement, and digital asset transactions. It is intended to derive relative value stability from a reserve framework referencing multiple fiat currencies and reserve assets.

ZEND is designed to minimise price volatility by reference to eligible cash, near-cash assets, sovereign debt instruments, money market instruments, regulated custodial accounts, and other high-quality liquid assets selected in accordance with Trnznd's treasury and liquidity policies.

However, ZEND does not carry a guarantee of value, liquidity, redemption, uninterrupted availability, or fixed market price.

2. No Guarantee of Value or Stability

Although ZEND is designed to be supported by reserve assets, Trnznd does not guarantee that ZEND will maintain any particular market value, exchange ratio, or trading price on secondary markets.

Users may suffer financial loss if the value of ZEND declines, if secondary market liquidity disappears, if redemption is delayed or unavailable, or if reserve assets are impaired.

3. Reserve and Backing Risk

Trnznd maintains reserve assets intended to support redemption obligations associated with outstanding ZEND. Reserve assets support Trnznd's contractual redemption obligations and do not necessarily create direct ownership rights, trust rights, fiduciary rights, bankruptcy-remote rights, safeguarded client asset status, or proprietary claims in favour of holders unless expressly required by applicable law.

Reserve assets may be held directly by Trnznd, through custodians, regulated investment structures, treasury management arrangements, affiliates, or service providers. References to segregation may refer to operational or accounting segregation and do not necessarily create bankruptcy remoteness or proprietary rights in favour of holders.

4. Reserve Impairment Risk

Reserve assets may be affected by market dislocation, sovereign default, interest rate changes, currency volatility, counterparty failure, custodian failure, banking disruption, liquidity stress, operational failure, legal restrictions, cyberattack, or force majeure events.

In extraordinary circumstances, Trnznd may implement temporary risk-management measures, including redemption delays, issuance suspensions, liquidity prioritisation procedures, treasury rebalancing measures, or temporary operational restrictions.

5. Currency Basket and Foreign Exchange Risk

ZEND is designed to reference a diversified basket of major global currencies rather than a single fiat currency. This diversified structure may reduce single-currency exposure, but it does not eliminate foreign exchange risk.

ZEND may rise or fall against any individual currency, including USD, EUR, GBP, JPY, CNY/CNH, or any other fiat currency. Users whose liabilities, accounting records, tax obligations, or commercial contracts are denominated in a single currency may experience gains or losses relative to that currency.

Nothing should be interpreted as a representation or guarantee that ZEND will maintain a fixed value against any specific sole currency in all market conditions.

6. Redemption Risk

Any right to redeem ZEND is a contractual right only and remains subject to compliance approval, sanctions screening, operational procedures, reserve availability, liquidity conditions, banking system functionality, blockchain functionality, and applicable law.

Only Eligible Users who have completed Trnznd’s onboarding, KYC, AML/CFT/CPF, sanctions screening, and other compliance procedures may directly mint or redeem ZEND with Trnznd.

Redemption requests may not be processed instantly and may be delayed, rejected, suspended, limited, reversed, queued, batched, or conditioned due to compliance reviews, banking delays, liquidity conditions, blockchain congestion, operational procedures, security controls, court orders, regulatory directives, sanctions restrictions, or force majeure events.

7. Liquidity and Secondary Market Risk

ZEND may not always be liquid or tradable. Secondary market liquidity may be limited, intermittent, fragmented, or unavailable. Markets may list or delist ZEND without notice, and an active market may never develop or may cease to exist.

Trnznd does not operate, control, guarantee, supervise, support, maintain, or influence secondary-market pricing, liquidity, settlement, market-making, exchange relationships, or trading availability. Users engaging in secondary-market transactions do so entirely at their own risk.

8. Smart Contract and Blockchain Risk

ZEND may operate across one or more blockchain networks, including Ethereum, Solana, Tron, and other supported protocols as Trnznd may designate from time to time.

Blockchain networks and smart contracts may experience bugs, vulnerabilities, outages, congestion, cyberattacks, validator failures, protocol changes, forks, governance disputes, exploitation, transaction reordering, failed transactions, delayed settlement, loss of access, or other technical failures.

No audit, code review, certification, or technical assessment can guarantee that a smart contract is free from defects, vulnerabilities, or future exploitability.

9. Cross-Chain and Bridge Risk

Where ZEND is made available across multiple blockchain networks, users may face additional risks relating to bridging, wrapped tokens, cross-chain messaging, liquidity fragmentation, chain-specific smart contract risk, transaction finality differences, and incompatibility between blockchain networks.

Trnznd may not support, recognise, redeem, reverse, or assume responsibility for wrapped, bridged, synthetic, derivative, or otherwise modified versions of ZEND created by third parties without Trnznd’s authorisation.

10. Wallet and Private Key Risk

Users are solely responsible for safeguarding their private keys, seed phrases, wallet credentials, devices, and access controls. Loss, theft, compromise, phishing, malware, unauthorised access, mistaken transfers, or incorrect wallet addresses may result in permanent and irreversible loss of ZEND.

Blockchain transactions are generally irreversible. Trnznd may be unable to recover, reverse, cancel, or compensate users for transactions sent to incorrect addresses, unsupported networks, compromised wallets, sanctioned wallets, smart contracts, or third-party platforms.

11. Cybersecurity Risk

The Trnznd platform, blockchain networks, wallets, exchanges, custodians, service providers, users, and counterparties may be exposed to cybersecurity threats, including hacking, phishing, malware, ransomware, denial-of-service attacks, private key compromise, smart contract exploits, social engineering, insider threats, or infrastructure failures.

Cyber incidents may result in loss of access, loss of ZEND, loss of data, delayed transactions, suspended platform functionality, unauthorised transfers, operational disruption, or financial loss.

12. Platform Availability and Operational Risk

The Trnznd platform, website, APIs, smart contracts, blockchain integrations, interfaces, valuation feeds, onboarding systems, compliance tools, payment rails, banking relationships, custodial systems, or other operational infrastructure may be unavailable, interrupted, delayed, suspended, modified, or discontinued.

Processing times for minting, redemption, transfer, verification, settlement, or other platform functions may vary due to compliance reviews, banking systems, liquidity conditions, blockchain congestion, external service providers, operational requirements, security controls, or force majeure events.

13. Compliance, KYC, AML and Sanctions Risk

Users may be required to complete identity verification, customer due diligence, source-of-funds verification, source-of-wealth verification, sanctions screening, wallet screening, transaction monitoring, and enhanced due diligence before accessing certain services.

Completion of verification procedures does not guarantee continued access to the platform or services. Trnznd may impose transaction limits, enhanced review, source-of-funds checks, wallet verification, account restrictions, delays, suspensions, or termination based on ongoing risk assessments, sanctions obligations, legal requirements, or internal compliance procedures.

Trnznd may refuse onboarding, reject transactions, block or restrict wallet addresses, report suspicious activity, cooperate with law enforcement, file regulatory disclosures, or take any action it considers necessary to comply with applicable law.

14. Freezing, Blocking and Enforcement Risk

Trnznd may freeze, blacklist, seize, restrict, report, suspend, or otherwise limit access to ZEND, wallet addresses, transactions, platform accounts, or associated assets where required by court order, regulatory direction, law enforcement request, sanctions obligations, applicable law, or internal compliance controls.

Where technically feasible and legally required, Trnznd may restrict or immobilise ZEND associated with sanctioned, unlawful, fraudulent, compromised, disputed, or prohibited activity.

15. Prohibited Use Risk

Users must not use ZEND or the Trnznd platform in connection with money laundering, terrorist financing, proliferation financing, sanctions evasion, fraud, tax evasion, market manipulation, cybercrime, ransomware, unauthorised activity, or any activity prohibited under applicable law.

Where Trnznd determines that a prohibited use has occurred, Trnznd may suspend or terminate access, freeze or blacklist wallet addresses, restrict transactions, report to competent authorities, cooperate with investigations, or take other action it considers appropriate.

16. Regulatory and Jurisdictional Risk

The legal and regulatory treatment of digital assets, stablecoins, tokenised settlement assets, payment tokens, e-money, securities, collective investment arrangements, payment services, deposit-taking activities, and related services is evolving and may differ significantly across jurisdictions.

Regulators, courts, tax authorities, central banks, government agencies, or other competent authorities may characterise ZEND or related activities differently from Trnznd's intended structure.

Users are responsible for determining whether they may lawfully acquire, hold, transfer, use, redeem, or otherwise deal with ZEND in their own jurisdiction.

17. Insolvency and Counterparty Risk

If Trnznd, a custodian, bank, reserve counterparty, payment processor, exchange, technology provider, liquidity provider, blockchain infrastructure provider, or other service provider becomes insolvent, fails, suffers disruption, acts improperly, or is subject to legal or regulatory action, users may experience delayed recovery, reduced recovery, loss of access, loss of value, or loss of assets.

In the event of insolvency, restructuring, administration, liquidation, or similar proceedings affecting Trnznd or related entities, holders may rank as unsecured creditors, experience delayed recovery, receive less than full value, or lose access to some or all associated value.

18. Custody and Third-Party Service Provider Risk

ZEND may be held through self-custody wallets or third-party wallets, exchanges, custodians, brokers, OTC desks, payment processors, or other platforms. Such third parties operate independently from Trnznd and may impose their own fees, restrictions, security practices, onboarding requirements, suspension rules, or transfer limitations.

Users who hold ZEND through a third party are exposed to that third party's operational, legal, cybersecurity, custody, insolvency, fraud, compliance, and contractual risks. Trnznd is not responsible for losses arising from the use of such third parties.

19. Valuation and Oracle Risk

Where ZEND issuance, redemption, risk controls, reserve reporting, or user interfaces rely on valuation inputs, Trnznd may use one or more valuation feeds, data sources, or price oracle mechanisms.

Valuation inputs may be stale, incorrect, interrupted, manipulated, unavailable, or affected by market disruption, data provider failure, system errors, latency, connectivity issues, or exceptional market conditions. Trnznd does not warrant that any valuation mechanism will be uninterrupted, error-free, complete, accurate, or reflective of secondary-market prices.

20. Fee, Cost and Spread Risk

Fees, spreads, charges, deductions, network fees, gas fees, banking fees, payment-processing costs, custody fees, foreign exchange costs, liquidity costs, treasury adjustment fees, operational processing fees, taxes, duties, levies, or third-party charges may apply to minting, redemption, transfer, settlement, or other services.

Applicable fees may vary depending on transaction size, jurisdiction, settlement method, currency, blockchain network conditions, liquidity conditions, counterparty risk, operational complexity, or other commercial factors. Fees may be modified in accordance with the Terms and applicable law.

21. Tax Risk

The tax treatment of acquiring, holding, transferring, using, redeeming, or disposing of ZEND may vary by jurisdiction and may change over time. Users may be subject to tax reporting, income tax, capital gains tax, withholding tax, VAT, GST, stamp duties, financial transaction taxes, exchange-control rules, or other obligations depending on their circumstances.

Nothing provided by Trnznd constitutes tax advice or a binding interpretation of Panamanian tax law or the tax law of any other jurisdiction. Users should obtain independent tax advice before engaging with ZEND or the platform.

22. Conflicts of Interest Risk

Trnznd, its affiliates, and related parties may maintain commercial, financial, operational, or contractual relationships with custodians, reserve managers, banking partners, payment processors, technology providers, liquidity providers, market makers, exchanges, compliance vendors, and other third-party service providers.

These relationships may create actual, potential, or perceived conflicts of interest. Trnznd may implement policies to identify, manage, and mitigate conflicts, but does not guarantee that all conflicts will be eliminated or fully disclosed unless required by applicable law.

23. Transparency and Disclosure Risk

Trnznd may publish reserve reports, attestations, proof-of-reserve statements, circulation metrics, asset allocation summaries, operational updates, or other disclosures. Such disclosures are for informational purposes only and do not constitute guarantees regarding solvency, liquidity, redemption, reserve sufficiency, or future performance.

Such information may rely on third-party service providers, may be updated, corrected, withdrawn, or revised, and may not be complete, accurate, timely, or continuously available.

24. Data Protection and Blockchain Transparency Risk

Blockchain transactions involving ZEND may be publicly visible, traceable, permanently recorded, accessible to third parties, and not capable of deletion or full anonymisation. Wallet addresses, transaction metadata, timestamps, balances, and transaction histories may be analysed using blockchain analytics tools.

Users should understand that blockchain-based systems may inherently limit privacy and that Trnznd cannot guarantee absolute privacy, confidentiality, or security of information transmitted through blockchain networks, third-party systems, or public distributed ledgers.

25. Amendment and Service Modification Risk

Trnznd may amend its Terms, policies, fee schedules, platform functionality, supported blockchain networks, reserve methodologies, operational processes, compliance requirements, or service availability from time to time.

Users who continue to use the platform or hold ZEND after the applicable effective date of revised terms may be deemed to have accepted the revised terms.

26. Force Majeure Risk

Trnznd may be unable to perform, delay performance, suspend services, restrict access, modify services, or fail to process issuance or redemption requests due to events beyond its reasonable control.

Force majeure events may include war, terrorism, civil unrest, cyberattacks, banking failures, payment network outages, blockchain outages, validator failures, protocol exploits, governmental actions, court orders, sanctions, pandemics, natural disasters, telecommunications failures, utility failures, data centre failures, labour disputes, or failures of third-party service providers.

27. No Fiduciary, Advisory or Agency Relationship

Trnznd acts as an independent contractual counterparty and technology-enabled service provider in connection with the issuance, administration, transfer, and redemption of ZEND.

No communication, statement, publication, interface, report, disclosure, or material provided by Trnznd constitutes investment advice, financial advice, tax advice, legal advice, accounting advice, fiduciary advice, or a recommendation to acquire, hold, transfer, redeem, or dispose of ZEND.

28. User Responsibility

Each user is solely responsible for understanding the risks of ZEND, safeguarding wallets and credentials, complying with applicable law, providing accurate information, maintaining appropriate records, satisfying tax obligations, verifying counterparties and wallet addresses, and determining whether ZEND is suitable for their own commercial, financial, legal, tax, operational, and risk-management purposes.

Users should seek independent professional advice before acquiring, holding, transferring, using, or redeeming ZEND, particularly where they are subject to regulatory, accounting, tax, treasury, fiduciary, sanctions, or reporting obligations.

29. Acknowledgement

By accessing the Trnznd platform, applying for onboarding, acquiring ZEND, holding ZEND, transferring ZEND, redeeming ZEND, or otherwise interacting with ZEND or the Trnznd services, each user acknowledges that:

1. They have read and understood this Risk Disclosure Statement.
2. They have read and understood the Relevant Information Document and the Terms and Conditions of Service.
3. They understand that ZEND involves legal, regulatory, technological, operational, liquidity, market, reserve, cybersecurity, counterparty, insolvency, tax, and other risks.
4. They understand that ZEND is not legal tender, not a bank deposit, not government-backed, not insured, and not guaranteed to maintain any particular value.
5. They understand that direct redemption is available only to Eligible Users and remains subject to compliance, operational, liquidity, reserve, legal, and technical conditions.
6. They are solely responsible for determining whether ZEND is lawful, suitable, and appropriate for their circumstances.
7. They accept the risks associated with accessing, holding, transferring, using, or redeeming ZEND.

30. Contact

For enquiries relating to this Risk Disclosure Statement, users may contact Trnznd through the official channels set out below.

Entity	Trnznd SA
Website	www.trnznd.io
Legal	legal@trnznd.io
Support and Complaints	support@trnznd.io