ANTI-MONEY LAUNDERING AND COUNTER-TERRORIST FINANCING POLICY

Maartandrise International Ventures Private Limited

Operating under the brand NodeRails

CIN: U70200DL2025PTC458055

Registered Office: 26/95, West Patel Nagar, New Delhi, Delhi 110008, India

https://noderails.com

Version 1.0 | Effective Date: 15 April 2026

Document Control

Document Title	Anti-Money Laundering and Counter-Terrorist Financing Policy
Legal Entity	Maartandrise International Ventures Private Limited (NodeRails)
CIN	U70200DL2025PTC458055
Date of Incorporation	13 November 2025
Registered Office	26/95, West Patel Nagar, New Delhi, Delhi 110008, India
Document Owner	Mohit Bhat, AML/CFT Compliance Officer
Approved By	Board of Directors of Maartandrise International Ventures Private Limited
Board Approval Reference	Board Resolution No: BR/2026/04/15/AML-CFT | Approval Date: 15 April 2026
Version	1.0
Effective Date	15 April 2026
Next Review Date	15 April 2027
Review Cycle	Risk-based; at minimum upon material business or regulatory change
Classification	Confidential; external sharing with partners and regulators on request

This policy sets out the AML/CFT standards adopted by Maartandrise International Ventures Private Limited and is intended for internal governance, partner due diligence, and compliance oversight purposes.

Table of Contents

Executive Summary

This document sets out the Anti-Money Laundering (AML) and Counter-Terrorist Financing (CFT) policy for Maartandrise International Ventures Private Limited, a company incorporated in India and operating globally under the brand NodeRails (the "Company").

NodeRails operates primarily as a technology and infrastructure provider and may work alongside regulated financial institutions, payment service providers, card issuers, virtual asset service providers, compliance providers, banking partners, blockchain programmes, and other licensed entities in delivering certain services. The Company develops software, wallet experiences, payment-link infrastructure, APIs, and financial technology products such as Wallcard that support secure, compliant, and scalable financial experiences for partners and end-users.

Custody of Funds. NodeRails operates a self-custodial payment infrastructure. NodeRails does not take custody of customer fiat or digital assets, maintain customer balances, or control users' private keys. Transactions are authorized directly by users from their own wallets, while settlement is performed through regulated banking and payment partners where applicable.

NodeRails maintains a risk-based AML/CFT framework aligned with international standards, including the Financial Action Task Force (FATF) Recommendations, and with applicable local laws and contractual obligations in the jurisdictions and arrangements in which it operates. The Company's governance model is designed to support partner compliance programmes, mitigate misuse of its platforms, and enable responsible innovation in payment, wallet, and virtual asset-related technology.

In integrated programmes, regulated partners may perform certain regulated functions, including customer onboarding, ongoing monitoring, and statutory suspicious transaction or activity reporting (STR/SAR), in accordance with their licences and applicable law. NodeRails cooperates with those partners through technical controls, contractual commitments, data availability, and escalation procedures, and undertakes direct regulatory reporting or registration only where required for its role in a particular arrangement.

This policy establishes NodeRails' enterprise AML/CFT standards and is intended for use in internal governance, partner due diligence, onboarding reviews, and compliance oversight by financial institutions, payment partners, card programmes, fintech counterparties, and compliance teams.

1. Policy Statement and Purpose

NodeRails is committed to supporting the prevention of money laundering, terrorist financing, sanctions evasion, proliferation financing, and related financial crime risks in connection with its products, services, and technology.

The Company acknowledges that its infrastructure and software may be used by regulated financial institutions and other organizations that have direct legal obligations under AML/CFT and sanctions laws. NodeRails seeks to design and operate its systems in a manner that supports those obligations and mitigates misuse.

The purposes of this policy are to:

- Set out NodeRails' internal AML/CFT governance framework, roles, and responsibilities appropriate for a global fintech technology provider.
- Describe the risk-based approach the Company applies to its customers (e.g., B2B clients, merchants, platforms) and to the design of its products, APIs, and wallet solutions.
- Establish principles for KYC/KYB information collection (where applicable), beneficial ownership transparency, sanctions and PEP screening, transaction-level risk controls, suspicious activity escalation, record-keeping, training, and cooperation with regulated partners and competent authorities.
- Define how NodeRails supports regulated partners in delivering compliant services and how the Company implements additional controls where required by law, regulation, licensing arrangements, or contractual obligations for its specific role.

This policy is a group-wide minimum standard for NodeRails. Where local AML/CFT or sanctions laws apply to the Company and are stricter than this policy, those local requirements prevail. Where NodeRails provides technology and infrastructure to a regulated entity, this policy operates in addition to, and does not replace, the partner's own AML/CFT framework.

2. Scope and Applicability

This policy applies to:

- Maartandrise International Ventures Private Limited, operating under the brand NodeRails, including its technology platforms, APIs, infrastructure, and user experiences such as Wallcard.
- All directors and officers of the Company.
- All employees, permanent or temporary, interns, contractors, and consultants who work on NodeRails products and services.
- Third-party service providers (e.g., KYC/KYB vendors, blockchain analytics providers, cloud providers, payment processors) to the extent they perform activities relevant to AML/CFT risk and where their services are engaged by the Company.

In particular, this policy covers:

- B2B customer relationships where NodeRails contracts directly with entities such as merchants, platforms, PSPs, or fintechs ("Customers").
- Technology and infrastructure used to facilitate or support payment, wallet, or virtual asset-related flows, typically operated in conjunction with licensed financial and payment partners.
- Any future NodeRails products that process, route, or support financial transactions or virtual assets as part of integrated solutions with regulated partners.

This policy documents NodeRails' enterprise AML/CFT standards as a global fintech technology provider and defines how the Company supports compliant use of its platforms in partnership with licensed financial institutions, payment service providers, card issuers, and other regulated counterparties.

3. Legal and Regulatory Framework

NodeRails' AML/CFT policy is principles-based and draws primarily from:

- FATF Recommendations, including the risk-based approach and guidance relevant to virtual assets, VASPs, payment services, and new technologies.
- Generally accepted financial crime risk management practices used by international banks, payment institutions, and compliant fintechs.
- AML/CFT and sanctions frameworks applicable to the Company's activities in jurisdictions where it has a meaningful operational nexus, to the extent those frameworks apply to its role as a technology and infrastructure provider.
- Partner and counterparty contractual requirements, including due diligence questionnaires, card scheme rules, and programme sponsor obligations.

The Company seeks to:

- Design its systems and processes to support partners' compliance with AML/CFT and sanctions obligations where NodeRails' technology is used in regulated payment or virtual asset flows.
- Align internal policies with applicable laws, licensing arrangements, and contractual duties that apply to NodeRails in respect of specific products, partnerships, and jurisdictions.
- Maintain accurate, role-appropriate compliance representations in partner onboarding, contractual documentation, and regulatory engagement.

This policy describes NodeRails' adopted AML/CFT standards and governance framework. Regulatory licensing status, reporting obligations, and the allocation of compliance responsibilities in any given arrangement are determined by applicable law and by the contractual structure between NodeRails and its regulated partners.

4. Definitions

Company: Maartandrise International Ventures Private Limited, operating under the brand NodeRails.

NodeRails / NodeRails Platform: The Company's core technology, infrastructure, APIs, SDKs, and related products, including Wallcard.

Customer / Merchant / Client: A legal entity or individual that contracts with the Company to use NodeRails' technology or infrastructure services.

Regulated Partner: A bank, financial institution, licensed payment service provider, card issuer, e-money institution, or regulated VASP/MSB that integrates with or relies on NodeRails technology to deliver regulated services.

End-User: An individual or entity that uses a product or service powered by NodeRails technology, typically onboarded and monitored by a Regulated Partner or Customer.

AML/CFT: Anti-money laundering and counter-terrorist financing measures as commonly understood under FATF standards and applicable national law.

Virtual Asset (VA): A digital representation of value that can be digitally traded or transferred and used for payment or investment purposes, as defined by FATF and relevant national frameworks.

Virtual Asset Service Provider (VASP): Any natural or legal person that conducts VA activities as a business on behalf of another person, as defined by FATF. References to VASPs in this policy support risk analysis, partner mapping, and programme design.

Risk-Based Approach (RBA): Calibrating the nature and intensity of AML/CFT measures to the level of money laundering and terrorist financing risk identified.

Beneficial Owner: The natural person(s) who ultimately own or control a Customer or on whose behalf a transaction is conducted, as defined under applicable law and FATF guidance.

PEP: Politically Exposed Person, as defined under applicable law and FATF guidance.

STR / SAR: Suspicious Transaction Report or Suspicious Activity Report filed with a competent authority or financial intelligence unit.

CDD / EDD: Customer Due Diligence and Enhanced Due Diligence.

Travel Rule: Obligations to exchange originator and beneficiary information with VA transfers, as implemented by regulated partners under FATF Recommendation 16 and local law.

5. Governance and Responsibilities

5.1 Board of Directors

The Board of Directors is ultimately responsible for overseeing the effectiveness of NodeRails' AML/CFT framework as appropriate for a technology-focused business whose services may be used in regulated financial contexts.

- Approves this policy and material amendments at appropriate intervals.
- Sets AML/CFT and sanctions risk appetite, including acceptable customer types, use cases, and geographies.
- Ensures appropriate resources (people, systems, data, and budget) to support AML/CFT responsibilities.
- Receives periodic updates on financial crime risk, key risk indicators, significant incidents, and material changes in the risk environment.

5.2 Executive Management

- Promotes a culture of integrity and financial crime risk awareness across engineering, product, operations, customer success, and commercial functions.
- Integrates AML/CFT and sanctions considerations into product design, architecture decisions, partner integrations, and operational processes.
- Ensures material financial crime risks and control gaps identified by the AML/CFT Compliance Officer are appropriately addressed.

5.3 AML/CFT Compliance Officer

The Company designates an AML/CFT Compliance Officer responsible for coordinating AML/CFT matters across the business. Currently, this role is held by Mohit Bhat, Director.

- Owns this policy and oversees its implementation, including periodic reviews and updates.
- Coordinates the enterprise-wide financial crime risk assessment.
- Monitors relevant developments in AML/CFT and sanctions standards and applicable local laws and partner requirements.
- Acts as the primary internal point of contact for AML/CFT topics, including coordination with regulated partners, counsel, and external advisors.
- Assesses partner requirements (e.g., banks, card issuers, PSPs, VASPs) and ensures NodeRails' controls and commitments are accurately reflected in contracts and documentation.

5.4 Other Personnel

Managers and team leads in relevant functions are expected to ensure workflows align with this policy and support the AML/CFT Compliance Officer in risk assessments and control implementation.

All employees and contractors must:

- Complete AML/CFT training appropriate to their role.
- Follow internal procedures regarding onboarding, monitoring, escalation, and data handling.
- Promptly raise any concerns or suspected misuse of the NodeRails platform for unlawful purposes.

6. Risk-Based Approach and Financial Crime Risk Assessment

6.1 Risk-Based Approach

NodeRails maintains a risk-based framework that recognizes its primary role as a technology and infrastructure provider and acknowledges that its platforms may be integrated into regulated financial flows operated by licensed partners and programme sponsors.

- Assessing ML/TF and sanctions risk across customer types, use cases, geographies, and products.
- Designing platform controls (data fields, risk flags, API events, analytics) that enable regulated partners to meet their obligations.
- Applying enhanced controls where higher-risk use cases are identified (e.g., certain cross-border, crypto, or high-velocity flows).

6.2 Enterprise-Wide Financial Crime Risk Assessment

The Company periodically conducts a financial crime risk assessment proportionate to its size and business model, identifying risks associated with customers, partners, products, APIs, and geographies; evaluating control effectiveness; and informing acceptance criteria and enhancements.

6.3 Risk Appetite and Prohibited Activities

NodeRails maintains zero tolerance for knowingly supporting activities that are clearly illegal, associated with serious financial crime, or subject to comprehensive sanctions.

The Company may decline or discontinue relationships or use cases involving, for example:

- Sanctioned individuals, entities, or comprehensively embargoed regions where exposure cannot be effectively controlled.
- Child sexual abuse material, human trafficking, narcotics trafficking, illegal arms dealing, or organized crime.
- Unlicensed or illegal gambling where prohibited.
- Fraud schemes, unlawful pyramid or Ponzi-type schemes, or unlicensed investment or FX services.
- Mixers, tumblers, or other tools primarily designed to obscure illicit fund flows, where such use is identified and cannot be mitigated.

A Restricted and Prohibited Use Cases list is maintained in Appendix A and may be updated by the AML/CFT Compliance Officer.

7. Customer and Merchant Due Diligence (KYC/KYB)

7.1 Customer Acceptance Principles

Where NodeRails maintains a direct contractual relationship with a Customer, the Company applies risk-based Customer Due Diligence (CDD) appropriate for a technology provider.

- Understanding entity identity, ownership, and key persons to mitigate misuse of its platform.
- Understanding the Customer's business model, products, target markets, and expected use of NodeRails infrastructure.
- Ensuring the Customer has appropriate regulatory status or partner structure for regulated activities (e.g., operating via licensed banks, PSPs, or VASPs).

Where licensed partners perform KYC/KYB on underlying end-users or merchants, NodeRails may rely on those partners' processes and focus due diligence on the partner relationship itself.

The Company may utilise third-party compliance and verification providers to support customer due diligence, identity verification, sanctions screening, beneficial ownership verification, and risk assessment activities. Such providers are selected and overseen on a risk-based basis, with appropriate contractual, data protection, and governance controls applied to their use.

7.2 Identification and Verification

For direct B2B Customers, NodeRails may collect and verify, on a risk-based basis:

- Legal entity name, registration details, and jurisdiction of incorporation.
- Registered and business addresses.
- Names and details of directors, key controllers, and authorized signatories.

- Ownership and control information, including beneficial owners where relevant.
- Information on business activities, primary products, and expected transaction patterns via NodeRails.

7.3 Beneficial Ownership

Where appropriate, NodeRails seeks to understand beneficial ownership and control of legal entity Customers, especially where structures are complex, involve higher-risk jurisdictions, or indicate opacity.

7.4 Risk Classification and Periodic Review

Customers may be assigned risk classifications (low, medium, high) based on sector, geography, volumes, transaction types, and crypto-related activities. NodeRails conducts periodic or event-driven reviews upon material changes in ownership, platform use, or adverse information.

7.5 Enhanced Due Diligence (EDD)

For higher-risk Customers and use cases, EDD may include:

- Additional information on ownership, governance, and key individuals.
- Sources of funds and wealth where the business model is complex or higher-risk.
- Independent checks using public sources, commercial databases, or due diligence providers.
- Confirmation of regulated partners, licensing status, or contractual arrangements with financial institutions.

7.6 Crypto-Specific Due Diligence and Partner Controls

Where NodeRails infrastructure is used in crypto or virtual asset contexts, NodeRails works with licensed VASPs, exchanges, custodians, and financial institutions that operate the regulated elements of those programmes. The Company focuses on assessing partner risk profiles and control frameworks, and may implement technical measures (e.g., exposure flags, address risk scoring) to support partner controls and programme integrity.

NodeRails' use of crypto-focused analytics and technical controls reflects its commitment to supporting partners' AML/CFT programmes and to mitigating misuse of its infrastructure in virtual asset-related flows.

8. Sanctions, Screening, and Watchlists

8.1 Sanctions Risk Management

NodeRails seeks to avoid knowingly facilitating activity that would breach applicable sanctions laws relevant to its operations and key partners' jurisdictions.

- Considering sanctions risk in customer and use-case acceptance.
- Integrating sanctions-related data from partners or third-party tools into risk views.
- Supporting partners' sanctions compliance via APIs, webhooks, and data fields.

- Suspending or limiting platform use where clear sanctions concerns arise, in coordination with partners and counsel.

8.2 PEP and Adverse Media Screening

For higher-risk relationships, NodeRails may screen Customer key individuals or beneficial owners against PEP and adverse media databases. Depending on the program structure, NodeRails and/or its regulated partners perform KYC/KYB, sanctions screening, and ongoing monitoring. Where regulated partners are responsible for onboarding, NodeRails supports these processes through technical controls, data sharing, and risk monitoring.

8.3 Internal Watchlists

NodeRails may maintain internal lists of rejected or exited counterparties and technical identifiers associated with known abuse, used to block or flag new relationships.

9. Transaction Monitoring and Ongoing Oversight

NodeRails focuses on monitoring platform usage and technical indicators rather than acting as the primary AML monitoring system for end-user transactions, which remains the responsibility of regulated partners.

- Rule-based or pattern-based monitoring to detect API abuse or conduct inconsistent with stated use cases.
- Blockchain analytics or similar tools for high-risk indicators in crypto-related flows visible to NodeRails.
- Logs, flags, and data exports to regulated partners to support their monitoring and investigations.
- Ongoing oversight of customer adherence to permitted use cases and contractual obligations.
- Assessment of new features and product changes for emerging financial crime risks.

10. Suspicious Activity Escalation and Cooperation

10.1 Internal Escalation

Employees must promptly escalate concerns about potential misuse to the AML/CFT Compliance Officer or designated channels, including unusual API usage, partner concerns, or adverse operational information.

10.2 Cooperation with Partners and Authorities

NodeRails generally does not act as the primary filer of statutory STRs/SARs in all jurisdictions.

- Cooperates with regulated partners by providing relevant data, logs, and technical support to enable their STR/SAR filings.
- Files or supports reports where NodeRails has a direct legal obligation for its limited role, in consultation with legal counsel.

- Responds to lawful information requests from competent authorities in accordance with applicable law and privacy requirements.
- Avoids tipping off where inconsistent with partner policies or applicable law.

11. Record Keeping and Data Protection

11.1 Record Keeping

NodeRails maintains records necessary to evidence B2B due diligence, support risk assessments and investigations, and enable partners to meet record-keeping obligations where NodeRails is a data source.

Retention periods are consistent with applicable legal requirements, contractual obligations, and the Company's data retention and privacy policies. Under India's PMLA framework, reporting entities are generally required to maintain certain records for at least five years; NodeRails aligns its retention practices with obligations that apply to its role and contracts.

11.2 Data Protection and Confidentiality

- Access to sensitive AML/CFT-related information is limited to personnel with a legitimate business need.
- Appropriate technical and organizational measures protect data from unauthorized access, alteration, or loss.
- Sharing with partners and vendors is governed by contracts, data processing agreements, and applicable privacy laws including India's Digital Personal Data Protection Act, 2023 where applicable.

12. Training and Awareness

NodeRails maintains a training and awareness programme including:

- Induction training on AML/CFT policy, ecosystem role, and reporting expectations.
- Periodic refresher training for product, engineering, operations, and customer-facing roles.
- Focused training for individuals with specific AML/CFT responsibilities.
- Coverage of ML/TF concepts, risk-based approach, prohibited use cases, and escalation procedures.

13. Independent Review and Continuous Improvement

NodeRails subjects its AML/CFT framework to periodic independent review commensurate with size, complexity, and risk profile. Reviews may be conducted by internal independent personnel or qualified external advisors and generate prioritized enhancement recommendations.

14. Breaches, Non-Compliance, and Consequences

- Investigation of alleged policy breaches or intentional platform misuse.
- Corrective actions to address control weaknesses.
- Disciplinary measures for employees or contractors who knowingly or negligently violate this policy.
- Termination or restriction of relationships with Customers or vendors posing unacceptable financial crime risk.

15. Exemptions and Conflicts

Material deviations require justification, documentation, and approval by the AML/CFT Compliance Officer and, where appropriate, Executive Management. Where this policy conflicts with applicable law or partner contractual requirements, the Company generally applies the stricter standard where reasonable and feasible.

16. Review and Document Management

This policy is reviewed periodically on a risk-based basis, and at minimum when:

- Material changes occur in products, risk profile, or partnerships.
- Significant developments arise in AML/CFT and sanctions standards.
- Material findings emerge from internal or external reviews.

17. Relationship to Partner Policies

This policy provides partners (such as banks, card issuers, PSPs, and VASPs) with visibility into NodeRails' AML/CFT governance framework, risk management approach, and financial crime controls as a technology provider operating in financial services ecosystems. It complements, not replaces, partners' own AML/CFT obligations. NodeRails may work with partners to map this policy to their due diligence requirements.

18. India Regulatory Context

Maartandrise International Ventures Private Limited is incorporated in India. NodeRails continuously evaluates the applicability of AML/CFT obligations under Indian law and relevant international frameworks as its products, partnerships, and operating model evolve.

India's Prevention of Money Laundering Act, 2002 (PMLA) and rules thereunder establish AML/CFT obligations for reporting entities as defined under applicable law and notifications. The scope of those obligations depends on the activities performed, the regulatory status of the programme, and the role NodeRails holds in a given arrangement.

Where required by law, regulation, licensing arrangements, or contractual obligations with regulated partners, NodeRails will implement appropriate controls, governance structures, reporting

procedures, registrations, and compliance measures. This may include, where applicable, appointment of a Principal Officer and Designated Director, registration with the Financial Intelligence Unit-India (FIU-IND), customer due diligence processes, record-keeping, and suspicious transaction reporting in accordance with PMLA requirements.

NodeRails supports regulated Indian and international partners in meeting their obligations where NodeRails technology forms part of their programmes and maintains internal standards designed to align with evolving FIU-IND guidance, RBI expectations where relevant to partner programmes, and global FATF-aligned practice.

19. Contact Information

General / Support	support@noderails.com
AML/CFT and Compliance Inquiries	compliance@noderails.com
AML/CFT Compliance Officer	Mohit Bhat, AML/CFT Compliance Officer
Privacy / Data Protection	privacy@noderails.com
Website	https://noderails.com
Wallcard Product	https://wallcard.noderails.com

Appendix A: Restricted and Prohibited Use Cases

The following list is illustrative and non-exhaustive. The AML/CFT Compliance Officer may update it based on risk assessments and partner requirements.

- Processing or facilitating transactions for comprehensively sanctioned jurisdictions or persons where sanctions cannot be mitigated.
- Services primarily designed to circumvent AML/CFT, KYC, or sanctions controls.
- Ransomware payment facilitation, darknet marketplaces, or stolen funds laundering.
- Unlicensed money transmission, unlicensed securities offerings, or unlicensed VASP activity where licensing is required.
- High-risk gambling without appropriate licensing and controls.
- Human trafficking, illegal narcotics, weapons trafficking, or terrorist financing.
- Child sexual abuse material or exploitation.
- Shell entities with no legitimate business purpose used to obscure ownership or activity.

Appendix B: Key AML/CFT Roles and Escalation Matrix

Scenario	First Response	Escalation
Suspected platform misuse	Employee / Manager	AML/CFT Compliance Officer
Partner raises financial crime concern	Account / Operations lead	AML/CFT Compliance Officer + Legal
Sanctions hit on B2B Customer	AML/CFT Compliance Officer	Executive Management; suspend access if warranted
Law enforcement / regulatory inquiry	AML/CFT Compliance Officer	Executive Management + Legal counsel
Material control failure	AML/CFT Compliance Officer	Board notification as appropriate

Board Approval and Signatures

This Anti-Money Laundering and Counter-Terrorist Financing Policy (Version 1.0) was reviewed and approved by the Board of Directors of Maartandrise International Ventures Private Limited with effect from 15 April 2026.

Board Resolution No: BR/2026/04/15/AML-CFT

Approval Date: 15 April 2026

Director Approval (on behalf of the Board)

I confirm that the Board of Directors of Maartandrise International Ventures Private Limited has approved this policy and that it represents the Company's adopted AML/CFT standards as a global fintech technology provider.

Name: Mohit Bhat, Director

Signature: _____

Date: 15 April 2026

AML/CFT Compliance Officer Attestation

I confirm that I am responsible for coordinating implementation of this policy across the business and for maintaining it under periodic risk-based review.

Name: Mohit Bhat, AML/CFT Compliance Officer

Signature: _____

Date: 15 April 2026

End of Document