

AML/CFT/CPF POLICY

Entity Name: Red Lane B.V.

Trading Name: Red Lane

Registered Address: Schottegatweg Oost 10, Unit 1-9 Bon Bini Business Center, Willemstad, Curaçao, Dutch Caribbean

Effective Date: 19 June 2026

Approved By: Kurason Trust Curaçao N.V. (Managing Director)

Authorized Representative: Mr. Jonathan Heymans

MLRO: Marika Dumbadze

Deputy MLRO: To be appointed

1. INTRODUCTION

This Anti-Money Laundering, Counter-Terrorist Financing and Counter-Proliferation Financing (AML/CFT/CPF) Policy establishes the internal framework of Red Lane B.V. to prevent, detect, and mitigate risks of money laundering, terrorist financing, and proliferation financing.

The policy is designed in accordance with Curaçao regulatory requirements and international standards and applies to all business activities, including:

- Online Casino Operations
- Sports Betting Services
- Live Casino Platforms
- Payment Processing Activities
- Cryptocurrency Transactions

This policy is binding on all employees, directors, contractors, and third-party service providers.

2. PURPOSE OF THIS POLICY

The purpose of this AML/CFT/CPF Policy is to ensure that Red Lane B.V.:

- Complies with all applicable Curaçao laws and regulations
- Implements a risk-based AML/CFT framework
- Prevents misuse of its platform for illicit financial activity
- Detects and reports suspicious activity
- Maintains strong governance and internal controls
- Meets all CGA licensing requirements

AML/CFT/CPF POLICY

3. REGULATORY FRAMEWORK

Red Lane B.V. complies with the following regulatory instruments:

3.1 Curaçao Legal Framework

- National Ordinance on Games of Chance (LOK)
- National Ordinance on Reporting of Unusual Transactions (NORUT)
- National Ordinance on Identification when Rendering Services (NOIS)

3.2 Regulatory Authority Requirements

- Curaçao Gaming Authority (CGA) AML/CFT/CPF Guidelines
- CGA Compliance Directives and Circulars
- Licensing conditions applicable to B2C gaming operators

3.3 International Standards

- Financial Action Task Force (FATF) 40 Recommendations
- FATF Risk-Based Approach Guidance
- United Nations Security Council Sanctions
- EU Sanctions Framework
- OFAC Sanctions Lists
- UK HM Treasury Sanctions List

4. AML/CFT/CPF GOVERNANCE FRAMEWORK

4.1 Governance Structure

Red Lane B.V. implements a **Three Lines of Defense Model**:

First Line of Defense

Operational teams responsible for:

- Customer onboarding (CDD)
- Transaction handling
- Initial risk identification

Second Line of Defense

Compliance function and MLRO responsible for:

- AML policy implementation

AML/CFT/CPF POLICY

- Monitoring and oversight
- STR evaluation and reporting
- Sanctions compliance

Third Line of Defense

Independent audit function responsible for:

- Annual AML audits
- Effectiveness testing
- Compliance assurance

4.2 Board Responsibilities

The Board of Directors is ultimately responsible for:

- Approval of AML/CFT/CPF Policy
- Establishing AML risk appetite
- Oversight of MLRO function
- Ensuring adequate resources for compliance
- Annual review of AML framework
- Ensuring regulatory compliance with CGA requirements

4.3 Senior Management Responsibilities

Senior Management is responsible for:

- Implementation of AML policies
- Ensuring operational compliance
- Supporting MLRO independence
- Ensuring staff training and awareness
- Managing AML-related risks

4.4 AML Risk Appetite Statement

Red Lane B.V. maintains a **LOW to MEDIUM risk appetite**, and explicitly:

- Does NOT accept sanctioned individuals
- Does NOT accept prohibited jurisdictions
- Applies strict controls to high-risk customers
- Monitors cryptocurrency exposure closely

AML/CFT/CPF POLICY

5. MONEY LAUNDERING REPORTING OFFICER (MLRO)

5.1 Appointment

MLRO: Marika Dumbadze

The MLRO is an independent compliance function reporting directly to senior management and the Board.

5.2 Responsibilities

The MLRO is responsible for:

- Receiving internal suspicious activity reports (SARs)
- Evaluating suspicious transactions
- Submitting STRs to FIU via goAML
- Maintaining AML records
- Liaising with CGA and FIU
- Overseeing AML training
- Conducting AML risk assessments

5.3 Deputy MLRO

A Deputy MLRO must be appointed to ensure:

- Continuity during MLRO absence
- Independent review of alerts
- Backup reporting capability

6. ENTERPRISE-WIDE RISK ASSESSMENT (EWRA)

Red Lane B.V. applies a structured **risk-based approach**.

6.1 Risk Categories

Customer Risk

- PEP customers
- High-value players
- Anonymous or inconsistent profiles

AML/CFT/CPF POLICY

Geographic Risk

- Turkey (primary market)
- FATF high-risk jurisdictions
- Sanctioned countries

Product Risk

- Casino games
- Sportsbook betting
- Live casino platforms

Payment Risk

- Credit/debit cards
- Bank transfers
- Cryptocurrency transactions

6.2 Risk Scoring Methodology

Risk Level	Score Range
Low	0–30
Medium	31–70
High	71–100

6.3 Risk Mitigation

- Enhanced Due Diligence (EDD) for high-risk customers
- Real-time transaction monitoring
- Sanctions screening systems
- Crypto wallet analysis tools

AML/CFT/CPF POLICY

7. CUSTOMER DUE DILIGENCE (CDD) FRAMEWORK

Red Lane B.V. implements a comprehensive Customer Due Diligence (CDD) framework in accordance with CGA AML/CFT/CPF requirements.

CDD is applied:

- At onboarding
- During account verification
- When transactions exceed thresholds
- When suspicion arises
- During periodic reviews

7.1 Customer Identification Requirements

All customers must provide:

Individual Customers:

- Full legal name
- Date of birth
- Nationality
- Residential address
- Email address
- Mobile number

Required Documents:

- Government-issued ID (passport / national ID card)
- Proof of address (utility bill / bank statement $\leq$ 3 months)
- Payment method verification (where applicable)

7.2 Verification Process

Red Lane B.V. applies a multi-layer verification process:

- Document authenticity checks
- Database verification (where available)
- Device and IP verification
- Behavioral pattern analysis
- Liveness/selfie verification (where applicable)

No account may be activated without successful completion of CDD.

AML/CFT/CPF POLICY

7.3 Customer Risk Classification

Each customer is assigned a risk rating:

Low Risk

- Verified identity
- Low transaction volume
- Non-PEP status
- Stable geographic profile

Medium Risk

- Moderate transaction activity
- Cross-border activity
- Increased deposit frequency

High Risk

- PEP status
- High-value transactions
- Crypto usage
- High-risk jurisdiction exposure

7.4 Customer Acceptance Policy

Red Lane B.V. will NOT onboard:

- Sanctioned individuals or entities
- Customers from prohibited jurisdictions
- Anonymous or fictitious users
- Customers refusing CDD requirements
- Shell companies without UBO disclosure

8. ONGOING MONITORING & PERIODIC REVIEW

CDD is not a one-time process.

8.1 Monitoring Requirements

Customer activity is continuously monitored for:

AML/CFT/CPF POLICY

- Transaction anomalies
- Behavioral changes
- Unusual betting patterns
- Rapid deposit/withdrawal cycles
- Third-party payment indicators

8.2 Periodic Review Cycle

Risk Level	Review Frequency
Low	Every 3 years
Medium	Every 2 years
High	Annually

8.3 Trigger Events for Review

Immediate review is required when:

- Large deposits or withdrawals occur
- Customer changes payment method
- Suspicious activity is detected
- Sanctions lists are updated
- Ownership structure changes

9. ENHANCED DUE DILIGENCE (EDD)

EDD is mandatory for high-risk customers.

9.1 EDD Trigger Conditions

EDD applies when:

- Customer is a PEP
- Customer is from a high-risk jurisdiction
- Transaction volumes are unusually high
- Cryptocurrency is used
- Complex ownership structure exists

9.2 EDD Requirements

Enhanced due diligence includes:

- Source of Funds (SoF) verification

AML/CFT/CPF POLICY

- Source of Wealth (SoW) verification
- Senior management approval
- Additional identity checks
- Enhanced transaction monitoring

9.3 EDD Documentation Requirements

Acceptable documents include:

Source of Funds:

- Salary slips
- Bank statements
- Business invoices
- Sale agreements

Source of Wealth:

- Tax returns
- Company ownership documents
- Investment portfolio statements
- Property sale contracts

10. POLITICALLY EXPOSED PERSONS (PEP) FRAMEWORK

10.1 Definition of PEPs

PEPs include:

- Foreign Politically Exposed Persons
- Domestic Politically Exposed Persons
- International Organization Officials
- Family members
- Close associates

10.2 PEP Screening Requirements

All customers must be screened against PEP databases:

- At onboarding
- During ongoing monitoring
- During periodic reviews

10.3 PEP Approval Requirements

AML/CFT/CPF POLICY

PEP relationships require:

- Senior Management approval
- Enhanced monitoring
- EDD completion
- Ongoing review every 12 months

11. ULTIMATE BENEFICIAL OWNER (UBO) IDENTIFICATION

11.1 Definition

A UBO is any natural person who:

- Owns 25% or more of shares
- Exercises control over the entity
- Has effective decision-making authority

11.2 Verification Requirements

UBO verification includes:

- Corporate registry extracts
- Shareholder registers
- Organizational structure charts
- Trust deeds (if applicable)

11.3 Failure to Disclose UBO

Where UBO cannot be identified:

- Account must NOT be activated
- Relationship must be rejected
- Suspicious activity report may be considered

12. CUSTOMER ONBOARDING CONTROLS

12.1 Onboarding Principles

Red Lane B.V. applies strict onboarding controls:

- No anonymous accounts
- No incomplete KYC acceptance
- No third-party accounts
- No proxy identity use

AML/CFT/CPF POLICY

12.2 Account Activation Rules

Accounts are activated only after:

- Full CDD completion
- Sanctions screening clearance
- Risk classification assignment
- Payment method verification

12.3 Rejection Criteria

Accounts must be rejected if:

- Identity cannot be verified
- Customer is on sanctions list
- Jurisdiction is prohibited
- Suspicious behavior is detected at onboarding stage

13. SANCTIONS COMPLIANCE FRAMEWORK

Red Lane B.V. maintains a strict sanctions compliance framework to ensure full adherence to international and local sanctions obligations.

13.1 Applicable Sanctions Lists

The Company screens all customers, transactions, and beneficial owners against:

- United Nations Security Council (UNSC) Sanctions List
- European Union (EU) Consolidated Sanctions List
- Office of Foreign Assets Control (OFAC – USA) List
- UK HM Treasury Sanctions List
- Other relevant national or regional sanctions lists

13.2 Sanctions Screening Process

Sanctions screening is conducted at:

- Customer onboarding
- Deposit transactions
- Withdrawal transactions

AML/CFT/CPF POLICY

- Account updates
- Periodic re-screening (ongoing monitoring)

Screening is automated where possible and supported by manual review.

13.3 Sanctions Match Handling Procedure

If a potential match is identified:

1. Account is immediately restricted
2. MLRO is notified without delay
3. Investigation is initiated
4. Customer activity is suspended
5. Regulatory reporting is conducted where required
6. Assets may be frozen pending investigation

13.4 Asset Freezing Requirements

Where sanctions are confirmed:

- Funds must be immediately frozen
- No withdrawals or transfers permitted
- Case escalated to regulatory authorities
- Full documentation retained

14. TRANSACTION MONITORING FRAMEWORK

Red Lane B.V. implements a risk-based automated transaction monitoring system.

14.1 Monitoring Scope

Monitoring covers:

- Deposits
- Withdrawals
- Bets and wagers
- Account transfers
- Bonus usage patterns
- Cryptocurrency flows

AML/CFT/CPF POLICY

14.2 Monitoring Scenarios

The system detects:

- Structuring (smurfing)
- Rapid in-and-out transactions
- Bonus abuse patterns
- Abnormal betting behavior
- Third-party payments
- Dormant account reactivation with large deposits

14.3 Risk-Based Thresholds

Risk Level	Monitoring Intensity
Low	Standard monitoring
Medium	Enhanced alerts
High	Real-time review

14.4 Red Flags in Transaction Monitoring

- Multiple deposits below threshold limits
- Frequent deposits with no gameplay
- Immediate withdrawal after deposit
- Use of multiple payment methods
- Transactions inconsistent with customer profile

15. SUSPICIOUS TRANSACTION REPORTING (STR)

15.1 Internal Reporting Process

All employees must report suspicious activity to the MLRO immediately.

Employee → Compliance Officer → MLRO

15.2 External Reporting

AML/CFT/CPF POLICY

The MLRO is responsible for reporting suspicious transactions to:

- Financial Intelligence Unit (FIU) Curaçao
- Via goAML reporting system

15.3 STR Submission Timeline

- STR must be submitted **without delay**
- No maximum threshold delay is permitted
- Urgent cases are escalated immediately

15.4 Tipping-Off Prohibition

Employees are strictly prohibited from:

- Informing customers of investigations
- Disclosing STR submission
- Providing any indication of suspicion

Violation may result in disciplinary action.

15.5 STR Record Keeping

All STR-related documentation must be retained for:

- Minimum of 10 years
- Including internal reports, decisions, and supporting evidence

16. TERRORIST FINANCING (TF) CONTROLS

Red Lane B.V. actively prevents misuse of its platform for terrorist financing.

16.1 TF Risk Indicators

- Transactions involving high-risk jurisdictions
- Unusual funding patterns
- Anonymous or inconsistent payment sources
- Links to sanctioned entities

AML/CFT/CPF POLICY

16.2 TF Monitoring Measures

- Enhanced transaction monitoring
- Continuous sanctions screening
- Behavioral analysis tools
- Customer risk profiling

17. PROLIFERATION FINANCING (PF) CONTROLS

17.1 PF Risk Definition

Proliferation financing includes funding related to:

- Weapons of mass destruction
- Dual-use goods
- Restricted military technologies

17.2 PF Controls

The Company implements:

- High-risk jurisdiction monitoring
- Sanctions screening integration
- Transaction anomaly detection
- Escalation to MLRO

17.3 PF Escalation Procedure

If PF risk is identified:

1. Immediate account freeze
2. MLRO investigation
3. Regulatory escalation
4. STR submission if required

18. ESCALATION MATRIX

Severity Level	Action
Low Risk Alert	Monitor

AML/CFT/CPF POLICY

Medium Risk Alert	Review by Compliance
High Risk Alert	MLRO escalation
Critical	Immediate freeze + STR consideration

19. CRYPTOCURRENCY AML/CFT FRAMEWORK

Red Lane B.V. permits the use of cryptocurrencies as a payment method and therefore applies enhanced AML/CFT controls to virtual asset transactions.

19.1 Accepted Virtual Assets

The Company accepts the following virtual assets:

- Bitcoin (BTC)
- Ethereum (ETH)
- Tether (USDT)

Additional assets may only be added following MLRO approval and risk assessment.

19.2 Crypto Risk-Based Approach

Cryptocurrency transactions are classified as **HIGH RISK by default**, unless mitigated by:

- Verified customer identity
- Clean blockchain history
- Low transaction volume
- Known exchange origin

19.3 Blockchain Monitoring Requirements

Red Lane B.V. utilizes blockchain analytics tools to:

- Trace transaction origin and destination
- Identify exposure to illicit services
- Detect mixing/tumbling services
- Monitor darknet-linked wallets
- Identify high-risk jurisdictions exposure

AML/CFT/CPF POLICY

19.4 Prohibited Crypto Activity

The following are strictly prohibited:

- Transactions via mixers or tumblers
- Privacy coins with anonymization features (if unsupported)
- Wallets linked to sanctioned entities
- Darknet marketplace exposure
- Untraceable peer-to-peer transfers without verification

19.5 Crypto Wallet Verification

Before accepting crypto deposits, the Company verifies:

- Wallet ownership (where possible)
- Exchange origin (regulated vs unregulated)
- Transaction history risk score
- Source of funds alignment

20. RECORD KEEPING & DATA RETENTION

20.1 Retention Policy

All AML/CFT/CPF-related records must be retained for a minimum period of:

10 (ten) years

20.2 Records to be Retained

The following records must be securely stored:

- Customer Due Diligence (CDD) files
- Enhanced Due Diligence (EDD) documentation
- Transaction history records
- Suspicious Transaction Reports (STRs)
- Internal compliance communications
- Sanctions screening results
- Training records
- Risk assessments (EWRA)

AML/CFT/CPF POLICY

20.3 Data Security Requirements

All AML data must be:

- Stored securely with restricted access
- Protected against unauthorized modification
- Encrypted where applicable
- Accessible only to authorized compliance personnel

20.4 Audit Trail Requirements

The Company maintains a full audit trail including:

- User login activity
- Transaction logs
- Changes to customer profiles
- Compliance decisions

21. AML TRAINING PROGRAM

21.1 Training Objectives

The AML training program ensures all employees:

- Understand AML/CFT obligations
- Identify suspicious activity
- Follow escalation procedures
- Comply with CGA requirements

21.2 Training Structure

Training is delivered in three categories:

1. Onboarding Training

- Mandatory for all new employees
- Covers AML fundamentals

2. Annual Refresher Training

- Updates on regulatory changes
- Case study analysis

AML/CFT/CPF POLICY

3. Role-Based Training

- MLRO-specific training
- Compliance officer training
- Customer support AML awareness

21.3 Training Content

Includes:

- AML/CFT/CPF fundamentals
- CDD/EDD procedures
- Sanctions compliance
- STR reporting process
- Cryptocurrency risks
- Red flag identification

21.4 Training Records

The Company maintains:

- Attendance logs
- Test results
- Certification records
- Training materials archive

22. INDEPENDENT AML AUDIT FRAMEWORK

22.1 Audit Requirement

An independent AML audit must be conducted:

At least once per year

22.2 Audit Scope

The audit covers:

- AML governance structure
- CDD/EDD effectiveness
- Transaction monitoring system
- STR reporting accuracy

AML/CFT/CPF POLICY

- Sanctions compliance effectiveness
- Training program adequacy

22.3 Audit Reporting

Audit results are submitted to:

- Senior Management
- Board of Directors
- MLRO

Findings must include:

- Identified weaknesses
- Risk ratings
- Corrective action plan

22.4 Remediation Requirements

All audit findings must be:

- Categorized by severity
- Assigned corrective actions
- Monitored until closure

23. THIRD PARTY & OUTSOURCING RISK MANAGEMENT

23.1 Outsourcing Principles

Where services are outsourced, Red Lane B.V. ensures:

- Full AML compliance of third parties
- Contractual AML obligations
- Ongoing monitoring

23.2 Due Diligence Requirements

Before onboarding any third party:

- Ownership structure must be verified
- AML controls must be assessed
- Regulatory history must be reviewed
- Risk classification must be assigned

AML/CFT/CPF POLICY

23.3 Ongoing Monitoring

Third parties are subject to:

- Annual AML reviews
- Performance monitoring
- Compliance audits

23.4 Prohibited Outsourcing

Outsourcing is NOT permitted where:

- AML responsibilities are fully delegated
- Transparency cannot be ensured
- Regulatory compliance cannot be verified

24. AML RISK APPETITE FRAMEWORK

24.1 Risk Appetite Statement

Red Lane B.V. maintains a **LOW to MEDIUM AML risk appetite** and explicitly avoids:

- Sanctioned individuals or entities
- High-risk jurisdictions without mitigation
- Anonymous or unverified customers
- High-risk crypto exposure without controls

24.2 Risk Acceptance Criteria

Risk is only accepted when:

- Adequate controls are in place
- Customer is fully verified
- Source of funds is validated
- Monitoring is effective

24.3 Risk Escalation Policy

Any deviation from risk appetite must be:

- Escalated to MLRO
- Approved by senior management
- Documented in compliance logs

AML/CFT/CPF POLICY

25. AML RED FLAGS & SUSPICIOUS INDICATORS

Red Lane B.V. maintains an extensive list of AML red flags to detect suspicious activity across all gaming and payment channels.

25.1 Customer Behaviour Red Flags

The following behaviours may indicate suspicious activity:

- Frequent deposits with no gameplay activity
- Immediate withdrawal after deposit
- Sudden increase in betting volume
- Repeated losses followed by large deposits
- Inconsistent personal or financial information
- Reluctance to provide KYC documents

25.2 Transaction-Based Red Flags

- Structuring transactions below reporting thresholds
- Use of multiple payment methods without justification
- Third-party deposits or withdrawals
- High volume transactions inconsistent with profile
- Circular movement of funds (deposit–withdraw–redeposit loops)

25.3 Account & Identity Red Flags

- Multiple accounts linked to same IP/device
- Use of VPN or anonymizing tools
- Mismatched identity documents
- Multiple accounts using same payment instruments
- Shared devices across multiple accounts

25.4 Geographic Red Flags

- Transactions from high-risk jurisdictions
- Attempts to mask location using VPN
- Frequent cross-border inconsistencies
- Access from sanctioned or prohibited regions

AML/CFT/CPF POLICY

25.5 Cryptocurrency Red Flags

- Use of mixers or tumblers
- Transfers from high-risk blockchain addresses
- Rapid conversion between crypto and fiat
- Transactions involving darknet-linked wallets
- Untraceable wallet funding sources

26. SUSPICIOUS TRANSACTION REPORTING (STR) FRAMEWORK

26.1 STR Identification Process

Suspicious activity is identified through:

- Automated monitoring systems
- Employee reporting
- Compliance reviews
- MLRO investigations

26.2 Internal Reporting Flow

The reporting chain is as follows:

Employee → Compliance Officer → MLRO

All staff must report suspicions immediately without delay.

26.3 MLRO Evaluation Process

The MLRO will:

- Review all alerts and internal reports
- Assess risk level and supporting evidence
- Determine whether STR submission is required
- Document decision rationale

26.4 External Reporting (FIU)

Where suspicion is confirmed:

- STR is submitted to FIU Curaçao
- Reporting is done via **goAML platform**

AML/CFT/CPF POLICY

- Submission is made without delay

26.5 Tipping-Off Prohibition

Employees are strictly prohibited from:

- Informing customers about investigations
- Disclosing STR submission status
- Alerting customers to monitoring activities

Violation of tipping-off rules may result in:

- Disciplinary action
- Termination
- Regulatory sanctions

26.6 STR Record Retention

All STR-related records must be retained for:

Minimum 10 years

Including:

- Internal reports
- MLRO decisions
- Supporting evidence
- Communication logs

27. ESCALATION FRAMEWORK

27.1 Risk Escalation Levels

Level	Description	Action
Level 1	Low risk alert	Monitor
Level 2	Medium risk	Compliance review
Level 3	High risk	MLRO escalation
Level 4	Critical risk	Immediate account freeze

AML/CFT/CPF POLICY

27.2 Immediate Freeze Conditions

Accounts must be immediately frozen when:

- Sanctions match is confirmed
- Strong suspicion of ML/TF exists
- Fraudulent identity is detected
- Regulatory instruction is received

27.3 Escalation Timeframes

- Level 3 alerts: same-day review
- Level 4 alerts: immediate action required
- STR filing: without delay

28. CUSTOMER REJECTION POLICY

28.1 Mandatory Rejection Criteria

Red Lane B.V. will reject onboarding of:

- Sanctioned individuals or entities
- Customers from prohibited jurisdictions
- Customers refusing identity verification
- Shell companies with no identifiable UBO
- High-risk customers without sufficient EDD completion

28.2 Discretionary Rejection Criteria

The Company may reject customers if:

- Risk profile exceeds acceptable threshold
- Inconsistent documentation is provided
- Behavioral indicators suggest ML/TF risk
- Payment methods cannot be verified

AML/CFT/CPF POLICY

29. AML PROGRAM EFFECTIVENESS & CONTROL TESTING

29.1 Effectiveness Testing

AML controls are tested to ensure:

- Detection accuracy
- Proper escalation
- Timely STR reporting
- Sanctions screening effectiveness

29.2 Key Performance Indicators (KPIs)

- Number of alerts generated
- STR submission rate
- False positive rate
- Time to escalation
- Audit findings closure rate

29.3 Continuous Improvement

The AML program is continuously improved through:

- Audit findings
- Regulatory updates
- MLRO feedback
- System enhancements

30. REGULATORY INSPECTION READINESS

30.1 Compliance Readiness Requirements

Red Lane B.V. maintains readiness for CGA inspections through:

- Complete AML documentation
- Audit trail availability
- Updated policies and procedures
- Staff training records

AML/CFT/CPF POLICY

30.2 Document Availability

The following must be immediately accessible:

- AML/CFT/CPF Policy
- EWRA reports
- CDD/EDD records
- STR logs
- Sanctions screening logs
- Training records

30.3 Regulatory Cooperation

The Company commits to:

- Full cooperation with CGA
- Timely submission of requested data
- Transparency in compliance operations

31. ANNEX A — CUSTOMER RISK SCORING MODEL

Red Lane B.V. applies a quantitative risk scoring methodology.

31.1 Risk Scoring Matrix

Risk Factor	Low (1)	Medium (2)	High (3)
Geography	EU/Low risk	Turkey	Sanctioned/high-risk
Customer Type	Verified individual	Corporate	PEP
Payment Method	Bank transfer	Card	Crypto
Transaction Size	Low	Medium	High
Behaviour	Stable	Moderate change	Suspicious

31.2 Risk Classification

AML/CFT/CPF POLICY

Total Score	Risk Level
5–8	Low Risk
9–12	Medium Risk
13–15	High Risk

32. ANNEX B — EDD CHECKLIST

Enhanced Due Diligence must include:

Identity Verification

- Valid passport or ID
- Proof of address

Financial Verification

- Source of Funds documentation
- Source of Wealth documentation

Additional Checks

- PEP screening
- Sanctions screening
- Adverse media screening
- Senior management approval

33. ANNEX C — SUSPICIOUS TRANSACTION REPORT (STR) TEMPLATE

STR Form Structure

- Customer Name
- Customer ID
- Account Details
- Date of Transaction
- Description of Activity
- Reason for Suspicion
- Risk Level
- Supporting Evidence
- MLRO Decision
- Date Submitted to FIU

AML/CFT/CPF POLICY

34. ANNEX D — ULTIMATE BENEFICIAL OWNER (UBO) DECLARATION FORM

Required Fields:

- Company Name : Red Lane B.V
- Registration Number : 149962
Jurisdiction : Curacao
- Ownership Structure : UBO - 100 % (Ugur Kartal) - (Kurason Trust Curacao N.V-managing Director)

Declaration:

We hereby confirm disclosure of all Ultimate Beneficial Owners (100 % ownership or control):

- Full Name : Ugur Kartal
- Date of Birth : 12.08.1997
- Nationality : Turkish
- Percentage Ownership - 100 %
- Source of Wealth - Personal investments, bank savings, business ownership and income from employment.

35. ANNEX E — AML TRAINING RECORD TEMPLATE

Training Log Includes:

- Employee Name
- Position
- Training Type
- Date Completed
- Score / Assessment Result
- Trainer Name
- Certification Status

AML/CFT/CPF POLICY

36. ANNEX F — SANCTIONS SCREENING PROCEDURE

Process:

1. Screen at onboarding
2. Continuous automated screening
3. Transaction-based screening
4. Periodic rescreening

Actions on Match:

- Freeze account
- Escalate to MLRO
- Investigate
- Report if required

37. ANNEX G — BOARD AML APPROVAL RESOLUTION

Board Resolution Text:

The Board of Directors of Red Lane B.V. hereby:

- Approves the AML/CFT/CPF Policy
- Confirms implementation of risk-based AML framework
- Appoints MLRO: Marika Dumbadze
- Mandates annual policy review
- Ensures full compliance with CGA, LOK, NORUT, and NOIS requirements

38. ANNEX H — AML CONTROL SUMMARY CHECKLIST

- Customer Due Diligence implemented
- Enhanced Due Diligence framework active
- PEP screening enabled
- UBO verification required
- Sanctions screening active
- Transaction monitoring system operational
- STR reporting process established
- MLRO appointed

AML/CFT/CPF POLICY

- AML training program active
- Independent audit scheduled annually

39. FINAL DECLARATION

Red Lane B.V. confirms that:

- This AML/CFT/CPF Policy is fully aligned with CGA regulatory requirements
- The Company adopts a risk-based AML framework
- All regulatory obligations under LOK, NORUT, and NOIS are implemented
- The Company maintains zero tolerance for money laundering and terrorist financing

40. POLICY REVIEW STATEMENT

This policy shall be:

- Reviewed annually
- Updated upon regulatory change
- Updated upon business model changes
- Approved by the Board of Directors

Signed by:

MLRO: Marika Dumbadze



Signed by

UBO: Ugur Kartal

