

Mr. Cedric Pietersz
Curaçao Gaming Authority
Scharlooweg 172-174
Willemstad-Curaçao

30 May 2025

Re: Uploading AML/CFT Policy

Dear Mr. Pietersz,

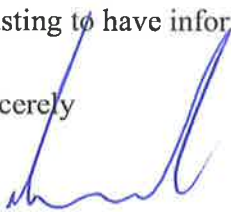
In order to comply with the due date for submission of the AML/CFT Policy, the applicant hereby uploads the draft version of the AML/CFT policy.

Note that this policy is not yet final as it is under review by management for approval and sign off.

Once approved, the final and official version will be signed off by management and uploaded to the portal. We expect this to take place in the course of the coming week.

Trusting to have informed you accordingly.

Sincerely



Raoul Behr
Managing Director

MoonRocket Holdings Ltd

Anti-Money Laundering & Combating the Financing of Terrorism ("AML/CFT") Policy

Last Update: May 2025
Version 1.5

Table of Contents

1. Introduction and Scope	8
Legal and Regulatory Framework	8
Scope.....	8
Our Approach	9
Implementation Note	9
2. Compliance Officer.....	9
Key Responsibilities.....	9
Independence and Authority	10
Operational Notes	10
3. Risk Assessment Framework	10
3.1 Business Risk Assessment (BRA).....	11
Assessment Process.....	11
Key Risk Areas We Monitor.....	11
Documentation and Approval	12
3.2 Customer Risk Assessment (CRA)	12
When CRA is Required	12
Risk Factors We Consider	12
Risk Categories.....	13
Real-Time Risk Scoring Integration	13
Practical Risk Override Scenarios.....	13
System Limitations and Workarounds.....	14
3.3 Customer Acceptance Policy (CAP)	14
When We Reject Customers	14
3.4 System Integration and Record Keeping.....	15
3.5 Technological Risk Assessment (New Products, Payments, or Delivery Channels). 15	
4. Customer Due Diligence (CDD).....	16
4.1 When We Perform CDD	16
4.2 Information We Collect and Verify	16
Basic Identity Information	16
Verification Process.....	17
Dual-System Verification Process	17
Common Verification Failures and Solutions	17
Document Authentication Red Flags (Manual Review Checklist).....	18
4.3 Sanctions and PEP Screening	18
4.4 Individual Customers Only	18
What We Do If We Detect Third-Party Activity.....	19
4.5 Understanding the Business Relationship	19
Progressive Source of Wealth Requirements	19

Affordability Reality Checks	20
4.6 Ongoing Monitoring	20
4.7 Record Keeping.....	21
4.8 Simplified Due Diligence (SDD).....	21
4.8.1 Conditions for Applying SDD	21
4.8.2 When SDD Is Strictly Prohibited	22
4.8.3 Oversight, Review, and Documentation.....	23
4.8.4 Internal Audit and Governance	23
4.9 Reliance on Third Parties for CDD	23
Practical Notes	23
<i>5. Enhanced Due Diligence (EDD)</i>	<i>24</i>
5.1 When We Apply EDD	24
Regulatory Risk Indicators.....	24
Operational Risk Indicators.....	24
5.2 Additional Measures for EDD Cases.....	24
Documentation Requirements	25
5.3 Account Restrictions During EDD.....	25
5.4 Ongoing Review of High-Risk Accounts.....	26
5.5 Management and Oversight.....	26
Practical Considerations	26
<i>6. Politically Exposed Persons (PEPs)</i>	<i>26</i>
6.1 Who We Consider PEPs	27
Foreign PEPs	27
Domestic PEPs	27
International Organization PEPs	27
PEP Family Members and Associates	27
6.2 How We Screen for PEPs.....	28
Screening Schedule	28
Data Sources	28
Screening Process.....	28
6.3 What Happens When We Find a PEP Match	28
6.4 Policy Rationale.....	29
6.5 Ongoing Monitoring	29
6.6 PEP Status Change - 30-Day Response Rule	29
6.7 Documentation and Oversight.....	30
<i>7. Sanctions Screening & Targeted Financial Measures.....</i>	<i>30</i>
7.1 Sanctions Lists We Monitor	30
7.2 Screening Process and Timing.....	31
Initial Screening.....	31

Ongoing Screening - Risk-Based Approach	31
7.3 Response to Sanctions Matches	32
7.4 Asset Freezing Procedures	33
7.5 Payment Partner Coordination	33
7.6 Prohibited Jurisdictions	33
7.7 Oversight and Quality Control	33
Operational Considerations	34
8. Ongoing Monitoring & Escalation Procedures	34
8.1 What We're Trying to Achieve	34
8.2 What We Monitor	35
Identity and Profile Changes	35
Transaction Patterns	35
Gaming Behavior	35
Account Relationships	35
Slack Alert Channels	36
Cross-Department Coordination Issues	37
8.3 How Our Monitoring Works	37
Automated Systems	37
Manual Review Process	37
When to File an ICR	39
ICR Process	39
8.5 Suspicious Transaction Reports (STRs)	39
STR Filing Requirements	39
STR Process	39
8.6 Documentation and Oversight	40
Operational Realities	40
9. Recordkeeping, Retention, and Audit Readiness	41
9.1 What Records We Keep	41
9.2 How Long We Keep Records	42
End-of-Life Data Handling	42
9.3 Storage Systems and Security	43
Technical Infrastructure	43
Access Controls	43
Data Integrity	43
9.4 Audit Preparation	43
Our Audit Readiness Process	43
9.5 Data Protection and Privacy	44
GDPR Compliance	44
Information Sharing	44
Staff Training and Confidentiality	44

Practical Considerations.....	45
Storage Costs.....	45
System Limitations.....	45
Operational Reality.....	45
10. AML/CTF Governance, Training, and Independent Review	45
10.1 Organizational Structure	45
Key Roles and Responsibilities.....	45
10.2 Policy Management and Updates	46
Review Schedule.....	46
Change Management Process.....	46
10.3 Staff Training Program.....	47
Training by Role	47
Training Content and Delivery.....	47
Training Compliance.....	47
10.4 Employee Screening	48
10.5 Internal Auditing and Testing.....	48
Internal Audit Program	48
External Audit	48
Performance Metrics	49
10.6 Management Reporting.....	49
Practical Considerations.....	49
Resource Constraints.....	49
Dual-Jurisdiction Complexity.....	50
System Dependencies.....	50
11. Cooperation with Authorities and Inter-Agency Communication	50
11.1 Legal Framework for Cooperation	50
11.2 Financial Intelligence Units (FIUs)	50
FIU Curaçao.....	50
FIU Estonia	51
Types of Cooperation.....	51
11.3 Curaçao Gaming Control Board (CGB).....	51
Regular Cooperation	51
Response Standards	52
11.4 Law Enforcement Cooperation	52
Safeguards and Procedures	52
11.5 Sanctions Authority Coordination	52
Immediate Reporting.....	52
Ongoing Coordination	52
Record Keeping.....	53
11.6 Data Protection in External Cooperation	53
Disclosure Documentation	53
11.7 Staff Training on Authority Cooperation.....	53

Operational Realities	54
Response Challenges.....	54
Communication Management.....	54
Practical Considerations.....	54
12. Breach Consequences and Enforcement Mechanisms	54
12.1 Who This Applies To.....	55
12.2 Types of Violations.....	55
Procedural Violations.....	55
Disclosure Violations.....	55
Negligence and Omissions	55
Management Failures.....	55
12.3 Consequences and Disciplinary Actions	56
Documentation and Tracking.....	56
12.4 Third-Party Violations	56
12.5 Self-Reporting and Whistleblowing	57
Self-Reporting Benefits.....	57
Whistleblower Protection.....	57
12.6 Remediation and Improvement	57
Root Cause Analysis.....	57
Corrective Actions	57
Follow-up and Monitoring	57
12.7 Regulatory Reporting.....	58
Reporting Process.....	58
Practical Considerations.....	58
Investigation Timelines.....	58
Resource Impact.....	58
Documentation Requirements	58
13. Use of Physical Establishments and White-Label Gaming Models	59
13.1 Pre-Launch Due Diligence on Physical/Partner Operators	59
13.2 Mandated Use of MoonRocket AML Systems and KYC Tools.....	59
13.3 Transaction Monitoring and Compliance Oversight	60
13.4 Staff Training and Certification	60
13.5 Mandatory Pre-Notification to the GCB.....	60
13.6 Termination of Non-Compliant Partners	60
14. Document Control, Ownership, and Certification	61
14.1 Document Information	61
14.2 Approval Process.....	62
14.3 Change Management	62
When Updates Are Needed.....	62
Update Process.....	62

Version History 62

14.4 Management Certification 63

14.5 Signature Page 64

1. Introduction and Scope

This Anti-Money Laundering and Counter-Terrorist Financing (AML/CFT) Policy applies to MoonRocket Holdings, including its subsidiaries MagicPoro Ltd and EastPoint Operations B.V. (referred to as "the Company" or "MoonRocket").

Since we operate gaming services under licenses in both Curaçao and Estonia, we need to comply with AML requirements in both jurisdictions. This means our policy is designed to meet the stricter requirements where they differ between the two jurisdictions.

Legal and Regulatory Framework

Our policy addresses the following regulatory requirements:

Curaçao:

- National Ordinance on Identification when Rendering Services (NOIS) (N.G. 2017 no. 92)
- National Ordinance on the Reporting of Unusual Transactions (NORUT) (N.G. 2017 no. 99)
- Sanctions National Ordinance (N.G. 2014 no. 55)
- Kingdom Sanction Act (N.G. 2016 no. 54)
- Regulations for combating Money Laundering, Financing of Terrorism and Proliferation of Weapons of Mass Destruction (January 2025) issued by the Curaçao Gaming Control Board (CGB)

International Standards:

- Financial Action Task Force (FATF) 40 Recommendations
- EU's 6th Anti-Money Laundering Directive (AMLD6)
- Caribbean Financial Action Task Force (CFATF) guidelines

Scope

This policy applies to all Company personnel involved in gaming or financial activities, including:

- Employees (full-time, part-time, contractors)
- Management and executives
- Consultants and agents
- Third-party service providers with access to customer data

The policy covers all products and services offered through our online platforms: online slots, live dealer games, sports betting, and related financial services.

Our Approach

We maintain a zero-tolerance approach to money laundering and terrorist financing. All staff are required to follow these policies and report suspicious activity through proper channels.

This policy is reviewed annually or when regulatory changes occur. The Curaçao Gaming Control Board may also require updates based on their supervisory activities.

Implementation Note

Given our dual-jurisdiction operations, some procedures may seem more complex than single-jurisdiction operators. This is intentional to ensure we meet the highest compliance standards across both licensing regimes.

2. Compliance Officer

The Company has appointed a dedicated Compliance Officer at senior management level to oversee our AML/CFT program. This position operates independently from gaming operations to ensure objective decision-making on compliance matters.

The Compliance Officer reports directly to the CEO and Board of Directors. The role is currently held by Olena Chaplytska.

Key Responsibilities

The Compliance Officer handles the following areas:

Policy and Procedures:

- Developing and maintaining our AML/CFT policies and procedures
- Reviewing and approving risk controls and monitoring systems
- Ensuring compliance with Curaçao NOIS/NORUT requirements and CGB regulations
- Staying current with regulatory changes in both jurisdictions

Customer Due Diligence:

- Overseeing Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) processes
- Monitoring customer transactions and behavior for suspicious patterns
- Making decisions on account restrictions, freezing, or closure

Regulatory Reporting:

- Preparing and submitting Suspicious Transaction Reports (STRs) to FIU Curaçao
- Maintaining secure records of all regulatory reports

- Coordinating with the Curaçao Gaming Control Board (CGB) and FIU Curaçao as needed
- Managing Internal Concern Reports (ICRs) and escalation procedures

Training and Oversight:

- Leading AML training programs for staff
- Conducting background screening for AML-relevant positions
- Organizing annual internal audits of our AML program
- Ensuring all compliance activities are properly documented

System Access:

- Full access to customer identification data and transaction records
- Access to all monitoring systems and alerts
- Authority to freeze accounts or restrict customer activity when required

Independence and Authority

The Compliance Officer operates independently and cannot be overruled by commercial considerations. All decisions regarding account freezing, STR submissions, or regulatory escalations are made by the Compliance Officer based on risk assessment and regulatory requirements.

The formal job description for this role is maintained on file and includes all duties and responsibilities outlined in this policy.

Operational Notes

Due to our dual-jurisdiction setup, the Compliance Officer must stay current with regulatory developments in both Curaçao and Estonia. This requires ongoing communication with regulators in both jurisdictions and may result in more complex procedures than single-jurisdiction operators typically maintain.

3. Risk Assessment Framework

Our AML/CFT program is built around a risk-based approach, as required by FATF recommendations and both Curaçao and Estonian regulations. This means we focus our compliance resources on higher-risk customers and transactions while applying simplified procedures for low-risk situations.

We evaluate ML/TF risks at two levels: across our entire business and for individual customers. All monetary amounts in this policy are stated in EUR (€), which is our primary operating currency.

3.1 Business Risk Assessment (BRA)

We conduct a comprehensive business risk assessment at least once per year. We also update it when significant changes occur, such as:

- Launching new gaming products or services
- Expanding into new markets or changing our customer acquisition approach
- Adding new payment methods (particularly cryptocurrency or high-risk payment providers)
- Regulatory changes in Curaçao, Estonia, or other relevant jurisdictions
- Serious compliance incidents or regulatory findings

Assessment Process

Our BRA covers the following areas:

Risk Identification - We identify potential ML/TF risks across:

- Customer segments and behavior patterns
- Payment methods and financial flows
- Affiliate and supplier relationships
- Product features and delivery channels
- Gaming verticals and betting patterns

Risk Analysis - We assess how likely each risk is to occur and what impact it could have on our business.

Risk Rating - Each area gets classified as Low, Medium, or High risk.

Control Assessment - We review our current controls and identify any gaps.

Key Risk Areas We Monitor

Risk Category	Examples
Customer Risk	PEPs, customers using third-party accounts, anonymous behavior
Geographic Risk	Customers from FATF high-risk countries or sanctioned jurisdictions
Product Risk	High-volume transactions without gameplay, bonus abuse patterns
Payment Risk	Prepaid cards, cryptocurrency, payment methods without proper verification

Channel Risk	Affiliate traffic from high-risk sources, account farming attempts
Technology Risk	Use of bots, VPNs to mask location, multiple account creation

Documentation and Approval

The final BRA report goes to our Board of Directors for annual approval. We keep detailed records of our findings and make the assessment available to the Curaçao Gaming Control Board (CGB), FIU Estonia, and our banking partners when requested.

The assessment incorporates findings from national risk assessments in both Curaçao and Estonia, plus FATF reports and EU guidance on high-risk countries.

While our Business Risk Assessment sets the strategic foundation for AML controls across MoonRocket, the true frontline of risk exposure happens at the customer level. The following Customer Risk Assessment (CRA) process allows us to evaluate each player's behavior, payment methods, and profile in real-time - before it becomes a threat to the platform.

3.2 Customer Risk Assessment (CRA)

Every customer gets a risk assessment based on their profile and activity. This determines what level of due diligence we apply.

When CRA is Required

Threshold Triggers:

- Curaçao license: When cumulative deposits reach €2,200 (equivalent to ANG 4,000)
- Estonian operations: €3,000 cumulative deposits under Estonian MLTFPA requirements
- MoonRocket policy: We apply the lower threshold of €2,200, or earlier if risk indicators are present

Other Triggers:

- Large single transactions approaching our thresholds
- Suspicious activity regardless of amount
- Concerns about previously collected customer information
- Requests from regulators or our banking partners

Risk Factors We Consider

- Customer identity verification and document quality
- PEP and sanctions list screening results
- Country of residence and payment method origins

- Expected vs. actual gaming and financial behavior
- Payment methods used (bank transfers are lower risk than prepaid cards or crypto)
- Unusual patterns like structured deposits or withdrawals without gameplay
- Source of funds clarity (required for higher-risk customers)

Risk Categories

Low Risk: Clear identity, regulated payment methods, consistent behavior matching their stated profile

Medium Risk: Remote verification only, non-EU documentation, unusual gaming patterns, limited information about source of funds

High Risk: PEPs, high-risk countries, heavy cryptocurrency use, multiple verification failures, previous suspicious activity reports

Real-Time Risk Scoring Integration

Our CRA operates on a dynamic scoring model that updates in real-time through SEON's API integration. The risk score calculation includes:

Base Risk Factors (Automated via SEON):

- Email domain risk (disposable emails = +15 points)
- Phone number carrier type (VOIP = +10 points)
- Social media presence (no digital footprint = +20 points)
- Device fingerprint anomalies (VPN/proxy = +25 points)
- Browser language vs declared country mismatch (+15 points)

Payment Method Risk Multipliers:

- Crypto deposits: 1.5x risk multiplier
- Prepaid cards: 1.3x risk multiplier
- Third-party payment methods detected via name mismatch: 2.0x multiplier
- Multiple payment methods in first 48 hours: 1.4x multiplier

Behavioral Risk Indicators (Tracked via Custom Dashboard):

- Deposits within 5 minutes of registration = High Risk flag
- Using max deposit limits repeatedly = Medium Risk flag
- Immediate max bet after deposit = Review trigger
- Login from 3+ countries in 24 hours = Automatic EDD

Practical Risk Override Scenarios

The Compliance team maintains override authority for system-generated risk scores when:

- Player provides LinkedIn profile showing legitimate high-income position
- Bank statements show consistent income supporting gambling activity

- Player is referred by existing VIP with clean history (still requires full KYC)

Note: All overrides logged in Slack #compliance-overrides channel with justification

System Limitations and Workarounds

Known Issues (as of last update):

- SEON API timeout issues during peak hours (19:00-23:00 CET) - fallback to manual review queue
- False positives on common names from high-risk countries - requires manual LinkedIn/Google search
- Crypto risk scores from Elliptic sometimes lag 2-4 hours - interim transactions held in review queue

Temporary Workaround Procedures: When automated risk scoring fails:

1. Transaction automatically routed to manual review queue
2. Alert posted to #aml-urgent Slack channel
3. Agent must complete review within 2 hours using backup checklist
4. If inconclusive, apply temporary withdrawal lock pending full review

3.3 Customer Acceptance Policy (CAP)

Based on the customer's risk level, we apply different procedures:

Risk Level	Onboarding	Verification Required	Ongoing Monitoring	Reporting
Low	Standard process	Basic KYC + sanctions/PEP check	Automated monitoring	None typically
Medium	Additional checks	Full KYC + address + source of funds declaration	Enhanced transaction monitoring	Internal review process
High	Senior approval required	Full KYC + proof of address + source of funds/wealth documentation	Real-time monitoring and manual review	Possible STR filing

When We Reject Customers

We cannot accept customers who:

- Cannot verify their identity satisfactorily
- Use third-party payment methods (violates our closed-loop policy)

- Are from countries on FATF, EU, or CGB blacklists
- Refuse to cooperate with our verification requirements

All exceptions to our standard acceptance criteria must be reviewed and approved by the Compliance Officer.

3.4 System Integration and Record Keeping

Customer risk profiles are integrated into our transaction monitoring and gaming systems. All risk assessments and supporting documentation are logged in our compliance systems.

Risk assessments are automatically updated when:

- Customers change their address, payment method, or identification documents
- New deposits over €500 or withdrawals over €1,000 occur
- Our monitoring systems detect unusual activity
- Documents expire or new sanctions/PEP matches are identified

We maintain all BRA and CRA records for at least 5 years after the customer relationship ends, as required by both Curaçao and Estonian regulations.

3.5 Technological Risk Assessment (New Products, Payments, or Delivery Channels)

MoonRocket conducts a **formal AML risk assessment** prior to launching any new product, payment method, or delivery mechanism that could affect exposure to ML/TF/PF risk. This includes:

- New games or product verticals
- New payment rails (e.g., crypto, wallets, EMIs)
- New onboarding processes (e.g., mobile-only, third-party apps)

The assessment includes:

- Risk and control mapping
- Potential abuse scenarios
- Documentation of mitigations
- Approval by the Compliance Officer

Each assessment is logged in the AML Governance Register and is reviewed within 3 months post-launch. If unanticipated risks arise, controls are updated or the feature is suspended.

4. Customer Due Diligence (CDD)

Our Customer Due Diligence procedures are designed to meet the requirements of both Curaçao and Estonian regulations, while following FATF standards and EU AML Directives. The goal is straightforward: verify who our customers are, understand why they're using our services, and monitor their activity for anything unusual.

CDD applies to all customers regardless of how they access our platform, with enhanced procedures for higher-risk situations.

4.1 When We Perform CDD

We conduct Customer Due Diligence in the following situations:

Trigger	Description
Deposit Thresholds	When cumulative deposits reach €2,200 (our standard threshold based on Curaçao requirements) or €3,000 within 180 days (Estonian requirements). We apply the €2,200 threshold across all operations.
Large Single Transactions	Individual transactions approaching €2,200, or withdrawal requests from customers who haven't played much
Suspicious Activity	Any amount where we see red flags or unusual patterns
Document Concerns	When we have doubts about previously collected information, expired documents, or data inconsistencies
Regulatory Requests	When requested by the CGB, FIU Estonia, our auditors, or banking partners

4.2 Information We Collect and Verify

When CDD is triggered, we collect and verify:

Basic Identity Information

- Full name (exactly as shown on government ID)
- Date of birth
- Nationality
- Place of birth
- Permanent home address

- National ID number (where available)
- Valid government-issued photo ID (passport, national ID, or driver's license)

Verification Process

- Document authentication through SumSub with biometric verification
- Address verification using utility bills or bank statements (not older than 3 months)
- Cross-checking through open banking connections (Brite, Tink) where possible
- IP/country consistency checks against provided documentation
- Document fraud screening through our fraud prevention partners like SEON

For low-risk customers, this basic verification is usually sufficient. Medium and high-risk customers may need to provide additional documents like employment confirmation or secondary ID.

Dual-System Verification Process

We run parallel KYC through both SumSub and SEON to maximize country coverage and reduce false rejections:

Primary Flow (SumSub):

- Covers 195 countries
- Average processing time: 3-5 minutes
- Auto-rejection rate: ~15%
- Biometric liveness detection active

Secondary Flow (SEON):

- Triggered when SumSub fails or for specific countries (Iran, Syria - auto-routed)
- Enhanced email/phone verification
- Social media correlation checks
- Processing time: 8-12 minutes

Manual Review Triggers:

- Both systems return "Uncertain" results
- Document quality score below 75%
- Facial recognition confidence below 85%
- Name variations exceed 2 characters
- Documents in scripts we can't verify (forwarded to external translation service)

Common Verification Failures and Solutions

Real issues we see daily:

1. **Glare on ID photos** - Customer service sends pre-written template with photo tips
2. **Expired documents** - System accepts up to 3 months expired during grace period (except for high-risk countries)

3. **Name mismatches** - Marriage certificates accepted for name changes
4. **Blurry selfies** - Automatic re-request with better lighting instructions

Response Templates stored in Zendesk:

- TEMPLATE_KYC_GLARE
- TEMPLATE_KYC_EXPIRED
- TEMPLATE_KYC_NAME_MISMATCH
- TEMPLATE_KYC_QUALITY

Document Authentication Red Flags (Manual Review Checklist)

Agents trained to spot:

- Font inconsistencies (especially common on fake Romanian IDs)
- Wrong hologram patterns (database of 50+ country samples)
- Photoshop artifacts around text/photos
- Invalid document numbers (checking algorithms for 28 countries)
- Misaligned text or borders

Weekly team meeting reviews new fraud patterns - recordings in Slack #kyc-fraud-patterns

4.3 Sanctions and PEP Screening

All customers are screened against relevant sanctions and PEP lists when they register and on an ongoing basis. We check:

- UN Consolidated Sanctions List
- EU Consolidated Financial Sanctions List
- US OFAC Sanctions Lists
- Kingdom Sanctions Act (Curaçao)
- Caribbean PEP Registry and other regional PEP databases
- Commercial databases (World-Check, Dow Jones Risk & Compliance)

Our screening is automated and updated daily. Any potential match triggers:

- Immediate account hold
- Internal Concern Report (ICR)
- Manual review by the Compliance Officer

We do not accept customers who appear on sanctions lists under any circumstances.

4.4 Individual Customers Only

Our platform is only available to individual persons acting on their own behalf. We do not allow:

- Legal entities or companies

- Trusts, syndicates, or pooled accounts
- Anyone acting on behalf of another person
- Use of third-party funds or shared payment methods

What We Do If We Detect Third-Party Activity

If we suspect someone is not the real account holder:

1. **Immediate account suspension**
2. **Internal Concern Report (ICR)** is filed
3. **Documentation request** for source of funds and identity of any other parties involved
4. **Investigation** to identify the real beneficial owner, including checking IP addresses, payment methods, email patterns, and linked accounts
5. **STR filing** with the relevant FIU if we identify high-risk individuals, sanctioned persons, or PEPs
6. **Account closure** unless the Compliance Officer determines there's no risk

This policy helps us avoid being used by hidden beneficial owners or organized betting syndicates.

4.5 Understanding the Business Relationship

We try to understand why customers are using our services by collecting information about:

- Their occupation and income level
- Whether they're casual players or more serious gamblers
- Expected activity levels (how much and how often they plan to play)
- Source of funds declarations

For higher-risk customers, we may request:

- Payslips, tax returns, or bank statements
- Employment confirmation
- Documentation for large deposits (asset sales, inheritance, legal settlements)

This information helps us establish what "normal" activity looks like for each customer.

Progressive Source of Wealth Requirements

Tier 1 (Up to €10,000 lifetime deposits):

- Self-declaration via dropdown menu
- No documentation required unless red flags

Tier 2 (€10,001 - €25,000):

- Enhanced declaration form
- Optional supporting documents increase withdrawal limits

Tier 3 (€25,000+ over rolling 6 months):

- Mandatory Source of Wealth documentation:
 - 3 months salary slips OR
 - Tax return OR
 - Business ownership docs OR
 - Investment portfolio statement
- Source of Funds for deposits over €5,000:
 - Bank statement showing salary credit OR
 - Crypto wallet history (analyzed via Chainalysis) OR
 - Sale contracts/inheritance documents

Escalation Timeline:

- Day 1: Automated email request
- Day 3: Personal email from VIP manager
- Day 7: Account limited to withdrawals only
- Day 14: Phone call attempt
- Day 30: Account suspended, remaining balance review

Affordability Reality Checks

Automated Flags (via internal analytics):

- Deposits exceeding 25% of declared monthly income
- Increasing deposit patterns over 3 months
- Credit card deposits followed by debit card (possible cash advance)
- Multiple failed deposits before successful one

Manual Review Indicators:

- Customer service complaints about "needing to win"
- Requests to increase limits repeatedly
- Playing continuously for 8+ hours
- Chasing losses pattern detected

Note: Responsible Gaming team notified via automated Slack integration for all affordability concerns

4.6 Ongoing Monitoring

CDD isn't just a one-time check. We continuously monitor:

- Daily transaction patterns for unusual volumes or behavior
- Changes in betting patterns or deposit sources
- Document expiration dates
- New sanctions or PEP matches (checked daily)

We require updated verification when customers:

- Change their address or country of residence
- Add new payment methods
- Show suspicious activity patterns
- Are requested by regulators

Our monitoring combines automated alerts with manual oversight by our AML team, supported by internal dashboards and case management systems.

4.7 Record Keeping

All CDD records are:

- Stored securely with access limited to Compliance, Legal, and senior management
- Kept for at least 5 years after the customer relationship ends or their last transaction
- Available immediately to the CGB, FIU Estonia, or authorized auditors

Our records include:

- All KYC/EDD documents submitted by customers
- Risk assessment logs and decisions
- Sanctions and PEP screening results
- All notes and correspondence related to verification

4.8 Simplified Due Diligence (SDD)

MoonRocket may apply Simplified Due Diligence (SDD) in strictly defined low-risk circumstances, in accordance with the Curaçao Gaming Control Board (GCB) Regulations (January 2025), the National Ordinance on Identification when Rendering Services (NOIS), and Financial Action Task Force (FATF) guidance.

We emphasize that **SDD is an exception** and may only be used where the **residual money laundering (ML), terrorist financing (TF), or proliferation financing (PF) risk is demonstrably low**. The Compliance Officer must approve each application of SDD based on documented criteria.

4.8.1 Conditions for Applying SDD

SDD may only be applied where **all** of the following conditions are met:

- The customer is a **natural person** acting in their own name (no third-party funding or legal entities).
- The customer's identity has been verified using a valid **government-issued photo ID** authenticated via biometric and anti-fraud tools.
- The customer **resides in a FATF-compliant jurisdiction** not flagged as high-risk by Curaçao, the EU, or FATF.

- The customer uses **regulated, traceable payment methods** (e.g. SEPA bank transfers, Finnish Trust Network).
- No matches or red flags exist on **sanctions, PEP**, or **adverse media** screening databases.
- The customer's lifetime cumulative deposits are **below €500** and show consistent, casual, non-suspicious activity.
- The customer's gameplay and financial behavior match a profile of **low-risk recreational use**.
- No anomalies are present in device fingerprinting, IP geolocation, or email/phone risk scoring.
- The customer has **not triggered** any internal monitoring alerts, risk thresholds, or manual review queues.

Each SDD application is documented in the customer's compliance profile and must be reviewed at least every **6 months** or immediately upon any risk escalation.

4.8.2 When SDD Is Strictly Prohibited

MoonRocket shall **not apply SDD under any circumstances** in the following situations:

- The customer is a **Politically Exposed Person (PEP)**, a close associate, or a family member of a PEP.
- The customer is from or transacts through a **high-risk country** listed by the FATF, EU, or Curaçao GCB.
- The customer uses **non-transparent or anonymous payment methods**, including:
 - Prepaid cards
 - Cryptocurrencies or virtual assets
 - Non-EU e-wallets or payment processors
 - Payment methods in names not matching verified identity
- The customer has previously failed verification or submitted questionable documentation.
- Structured deposits near €2,200 or €5,000 thresholds suggest an attempt to avoid CDD.
- The customer uses **VPNs, proxies, or TOR browsers**, or their activity is flagged as bot-like or coordinated.
- The customer engages in **high-volume play**, inconsistent with self-declared income or expected behavior.

SDD is also **automatically disabled** if:

- A new payment method is added.
- A withdrawal request exceeds €200.
- An Internal Concern Report (ICR) is opened.
- An updated sanctions list generates a new match or partial match.

4.8.3 Oversight, Review, and Documentation

All SDD approvals must be:

- Reviewed and signed off by the Compliance Officer before activation.
- Logged in the centralized **SDD Register** with justification and expiry date.
- Subject to **semi-annual review** or immediate review upon behavioral change.

Customers granted SDD are tagged in the compliance system and **automatically upgraded** to standard CDD or EDD if their risk profile increases. The transition is logged, and the customer is notified if additional documentation is required.

4.8.4 Internal Audit and Governance

- The Compliance Committee reviews all active SDD cases quarterly.
- The internal audit team tests a random sample of SDD cases every 6 months.
- Any improper SDD usage is escalated to senior management and remediated.

4.9 Reliance on Third Parties for CDD

MoonRocket does not delegate core AML responsibilities. However, we may rely on regulated third parties (e.g., KYC vendors like SumSub) for collecting and verifying documents, subject to:

- Immediate access to full CDD data
- Written contracts in place
- Assurance that the third party is regulated and AML-compliant

MoonRocket retains full accountability for:

- Risk assessments
- Monitoring
- STR filings

All third-party reliance arrangements are reviewed annually. Any failure in service performance results in withdrawal of reliance approval.

Practical Notes

Due to our dual-jurisdiction operations, some customers may find our verification requirements more extensive than other operators. This is necessary to ensure we meet the highest standards across both Curaçao and Estonian regulatory frameworks.

Processing times for verification may vary depending on document quality, customer responsiveness, and current workload. We aim to complete standard verifications within 48-72 hours of receiving complete documentation.

5. Enhanced Due Diligence (EDD)

Not every customer fits neatly into standard risk profiles. In our experience, higher-risk players often attempt to exploit gray zones: fast deposits via crypto, playing without meaningful gameplay, or sudden spikes in volume from unlikely regions. This is where Enhanced Due Diligence (EDD) comes into play - our second layer of defense.

Enhanced Due Diligence goes beyond our standard Customer Due Diligence procedures. We apply EDD when customers or transactions present higher than normal money laundering or terrorist financing risks. This involves more thorough investigation, additional documentation requirements, and closer ongoing monitoring.

EDD is required by FATF standards, EU AML Directives, and both Curaçao CGB and Estonian FIU regulations for higher-risk situations.

5.1 When We Apply EDD

We trigger Enhanced Due Diligence in the following situations:

Regulatory Risk Indicators

- Customer lives in or sends money from a country on FATF or EU high-risk lists
- Customer is identified as a Politically Exposed Person (PEP) or is related to/associated with a PEP
- Customer appears on sanctions lists or in adverse media reports
- Transaction patterns that don't match the customer's stated profile or expected behavior

Operational Risk Indicators

- Deposits exceeding €5,000 in any 30-day period, or €10,000 lifetime, especially through non-bank payment methods
- Heavy use of cryptocurrency with concerning risk scores (Chainalysis score above 75)
- Structured deposits that appear designed to avoid our thresholds with little or no actual gameplay
- Multiple attempts to circumvent limits through different accounts or altered personal information
- Refusal to cooperate with standard verification or suspicious documentation

The Compliance Officer may also initiate EDD proactively for testing purposes or when patterns seem unusual even if they don't meet specific triggers.

5.2 Additional Measures for EDD Cases

Enhanced Due Diligence involves deeper investigation than standard CDD:

Category	Enhanced Requirements
Identity Verification	Second form of ID; selfie with document and current date; enhanced biometric verification
Address Confirmation	Multiple sources (utility bill + bank statement + address verification service)
Source of Funds	Payslips, tax returns, bank statements, or dividend confirmations
Source of Wealth	Documentation of asset sales, inheritance, business income, or investment records for significant wealth
Transaction Review	Detailed analysis of deposits, withdrawals, gameplay patterns, and account behavior
Enhanced Screening	Manual verification of sanctions/PEP matches, secondary database checks, adverse media searches
Management Review	Compliance Officer approval required; detailed decision documentation; possible escalation to senior management

Documentation Requirements

Every EDD case gets:

- A dedicated case file with all supporting documents
- Clear documentation of our decision (approve with monitoring, approve with restrictions, or reject)
- Record of any account limitations (deposit caps, withdrawal restrictions, account suspension)

5.3 Account Restrictions During EDD

While we're conducting Enhanced Due Diligence:

- **Deposits and gameplay** can usually continue at reduced limits unless there's a sanctions or PEP match
- **Withdrawals are typically restricted** until we complete our review and verify all required information
- If the customer doesn't respond or provide complete information within **30 days**, we mark the account as non-compliant and suspend it
- Any held funds can only be returned to the original funding source after our risk review

If we can't resolve money laundering or terrorist financing concerns:

- We file a Suspicious Transaction Report (STR) with the appropriate FIU
- The customer account may be permanently closed with full documentation retained for regulatory review

5.4 Ongoing Review of High-Risk Accounts

Customers flagged as high-risk or subject to EDD get regular re-reviews:

- **Active accounts:** Reviewed quarterly
- **Immediate review** when there are significant changes (new documents, payment methods, unusual activity spikes)
- Any changes in risk status must be approved and documented by the Compliance Officer

5.5 Management and Oversight

- All EDD cases are tracked in our internal case management system
- The Compliance Officer oversees all EDD activity and conducts random quality checks on closed cases
- We prepare periodic effectiveness reviews for senior management
- EDD procedures are updated annually or when regulations change, audit findings require it, or new money laundering patterns emerge

Practical Considerations

EDD cases typically take 5-15 business days to complete, depending on:

- Customer responsiveness in providing requested documents
- Complexity of the customer's financial situation
- Need for additional verification from external sources
- Current case load in our compliance department

Customers subject to EDD are notified about additional requirements and potential delays. We aim to complete reviews as quickly as possible while ensuring thoroughness.

Due to our operations in both Curaçao and Estonia, some EDD requirements may seem more extensive than other operators, but this ensures we meet the highest regulatory standards across both jurisdictions.

6. Politically Exposed Persons (PEPs)

Politically Exposed Persons present higher money laundering risks due to their positions and potential access to public funds. Our approach to PEPs follows requirements from Curaçao

CGB regulations, EU AML Directives (AMLD4-6), Estonian AML Act, and FATF Recommendations 12 and 22.

We take a strict approach to PEP relationships. When we identify a PEP, we do not accept them as customers. This policy helps us avoid the complex ongoing monitoring and enhanced due diligence that PEP relationships would require.

6.1 Who We Consider PEPs

A Politically Exposed Person is someone who holds or has held a prominent public position, either domestically or internationally.

Foreign PEPs

- Heads of state or government (presidents, prime ministers)
- Senior politicians (cabinet ministers, members of parliament)
- Senior government, judicial, or military officials
- Central bank board members and senior officials
- Ambassadors and consuls
- Senior executives of state-owned enterprises

Domestic PEPs

- Individuals holding similar positions within Curaçao, Estonia, or countries where we have significant operations

International Organization PEPs

- Directors, deputy directors, and board members of international organizations like the UN, NATO, WHO, World Bank, IMF

PEP Family Members and Associates

We also treat the following as PEPs:

Immediate Family:

- Spouse or domestic partner
- Children and their spouses
- Parents

Close Associates:

- Known business partners or co-owners of legal entities with the PEP
- People with close financial or social relationships to the PEP
- Anyone who appears to be a beneficial owner of transactions where the PEP makes decisions

6.2 How We Screen for PEPs

Screening Schedule

- **At registration:** All customers screened through our third-party compliance system before allowing any deposits or gameplay
- **Database updates:** When our screening provider updates their PEP databases (typically monthly), we automatically receive alerts for any existing customers who now match new entries
- **Event-triggered screening:** When customers update personal information, add payment methods, or reach significant transaction milestones
- **Risk-based periodic screening:**
 - **High-risk customers** (crypto users, high deposit volumes): Every 6 months
 - **Medium-risk customers** (cross-border payments, higher activity): Annually
 - **Low-risk customers** (verified EU customers, consistent low activity): Every 2 years or upon significant activity changes

Data Sources

We use multiple screening sources:

- UN, EU, OFAC, and Kingdom Sanctions Act lists
- Commercial databases (World-Check, Refinitiv, Dow Jones Risk & Compliance)
- Government registries and adverse media searches
- Regional databases including Caribbean PEP Registry

Screening Process

Our system checks customer names, dates of birth, nationalities, and document numbers against PEP databases. The system uses fuzzy matching to catch variations in names and includes alias checking.

Screening results are classified as:

- **False positive:** Clear mismatch, no action needed
- **Potential match:** Requires manual review
- **Confirmed match:** Verified PEP identification

6.3 What Happens When We Find a PEP Match

When our screening identifies a potential or confirmed PEP:

1. **Immediate account freeze** - Customer cannot deposit, withdraw, or place bets until we complete our review
2. **Internal Concern Report (ICR)** - We create a formal internal report documenting the match, customer details, and account status

3. **Manual verification** - The Compliance Officer reviews the match to determine if it's accurate
4. **Decision and action:**
 - **Confirmed PEP:** Account is permanently closed
 - **Unverified but likely:** Account remains suspended pending further investigation
 - **False positive:** Account restrictions are lifted with documentation
5. **Record keeping** - We maintain full documentation of our review process, decision rationale, and any communications for at least 5 years
6. **Regulatory reporting** - If we have grounds to suspect money laundering or terrorist financing, we file an STR with the relevant FIU

6.4 Policy Rationale

We don't make exceptions to our PEP policy. This means:

- No PEP relationships regardless of transaction amounts or risk level
- No different treatment for "low-risk" or former PEPs
- The policy applies even for small deposits

This approach eliminates subjective decision-making and ensures consistent application. It also removes commercial pressure from compliance decisions.

6.5 Ongoing Monitoring

PEP status can change after customer onboarding, so we maintain ongoing screening. Additional PEP checks are triggered by:

- Address or nationality changes
- New payment methods
- Significant increases in deposit or withdrawal activity
- Staff reports or external notifications

If we discover that an existing customer has become a PEP, we apply the same review and closure process within 30 days of identification, as required by Curaçao regulations.

6.6 PEP Status Change - 30-Day Response Rule

In line with Curaçao GCB AML Regulation, if an existing customer is later identified as a PEP, MoonRocket must act within **30 calendar days** of the date of detection. Required steps:

1. Freeze the account immediately
2. Open an Internal Concern Report (ICR)
3. Review the relationship and source of funds
4. Decide and execute closure or STR escalation

All actions are logged in the PEP case file. Oversight is performed by the Compliance Officer and Legal. Any delay beyond 30 days requires CEO notification and internal breach review.

6.7 Documentation and Oversight

- All PEP screening results are logged in a secure database accessible only to compliance staff
- The Compliance Officer reviews and approves all PEP match determinations
- Monthly PEP screening reports are reviewed by the CEO or designated Board member
- All match investigations are retained in our centralized ICR system
- We review PEP policy effectiveness annually or when regulations change

Operational Notes

Our PEP screening may identify more potential matches than some operators due to our comprehensive database coverage and conservative matching criteria. This is intentional to ensure we don't miss any genuine PEP relationships.

Processing PEP reviews typically takes 2-5 business days depending on the complexity of verification required. During this time, affected accounts remain frozen to prevent any unauthorized activity.

Customers who are incorrectly flagged as PEPs will have their accounts restored quickly once we complete verification, but we prefer to err on the side of caution with initial screening.

7. Sanctions Screening & Targeted Financial Measures

We maintain a comprehensive sanctions compliance program to detect and prevent any activity involving individuals, entities, or jurisdictions subject to international sanctions. This is a legal requirement under Curaçao, Estonian, EU, and international sanctions regimes.

Sanctions compliance is non-negotiable. A confirmed match results in immediate account suspension, asset freezing, and mandatory reporting to relevant authorities.

7.1 Sanctions Lists We Monitor

Our third-party screening system monitors the following sanctions lists with automatic updates:

Source	List Coverage
--------	---------------

United Nations	UN Security Council Consolidated List
European Union	EU Consolidated Sanctions List
United States	OFAC SDN List, Non-SDN Lists (CAPTA, FSE, etc.)
United Kingdom	OFSI Consolidated List
Netherlands/Curaçao	Kingdom Sanctions Act Designations
Estonia	National Financial Sanctions List
Additional Sources	FATF high-risk countries, internal watchlists

Our screening covers customer names, aliases, dates of birth, nationalities, document numbers, and payment method geographic indicators.

7.2 Screening Process and Timing

Initial Screening

- **At registration:** All customers screened before account activation
- **At first financial transaction:** Additional screening when customers make their first deposit or withdrawal request

Ongoing Screening - Risk-Based Approach

Manual Database Checks for New Sanctions:

- When sanctions lists are updated (typically weekly), we receive notifications of newly added sanctioned persons and entities
- Our Compliance Officer manually searches our customer database for any matches against the new sanctions entries
- This manual process ensures we identify any existing customers who may match newly sanctioned individuals
- Any potential matches found are immediately flagged for review and potential account freezing

Event-Triggered Screening:

- New or changed payment methods (especially new bank accounts, cards, or crypto addresses)
- Changes to personal information (address, name, nationality, documents)
- Manual escalations through Internal Concern Reports (ICRs)

Periodic Re-Screening Based on Risk Level:

Risk Level	Screening Frequency	Criteria
High-Risk	Every 3 months	Large depositors, crypto users, customers from elevated-risk countries, frequent travel patterns
Medium-Risk	Every 6 months	Cross-border payments, non-EU documents, moderate activity levels
Low-Risk	Annually	Verified EU customers, consistent low-risk behavior, domestic payment methods

This risk-based approach ensures we focus resources where sanctions risks are highest while maintaining cost-effective operations.

7.3 Response to Sanctions Matches

When our screening system identifies a potential sanctions match:

1. **Immediate account freeze**
 - Customer access blocked automatically
 - All account funds frozen in place
 - No deposits, withdrawals, or gameplay permitted
2. **Internal escalation**
 - Internal Concern Report (ICR) created automatically
 - Compliance Officer notified immediately for manual review
3. **Match verification**
 - Manual review to confirm if it's a true match or false positive
 - Documentation of decision rationale
4. **Regulatory reporting**
 - **Curaçao:** Report to FIU Curaçao and notify the CGB
 - **Estonia:** File with FIU Estonia and Sanctions Supervisory Authority
 - **US-related:** Consider OFAC voluntary disclosure if US persons or USD involved
5. **Documentation**
 - All records retained for 5 years minimum
 - Complete decision trail including match details, customer profile, communications, and supporting evidence

We've had real cases where customers flagged by our sanctions engine turned out to be innocent travelers with name similarities. In each instance, a manual review prevented both wrongful exclusion and risk exposure. Every match - false or not - is documented and escalated in line with our zero-tolerance framework.

7.4 Asset Freezing Procedures

We follow mandatory asset freezing requirements under both Curaçao and EU law:

- Funds frozen immediately without prior notice to the customer
- No partial withdrawals or fund transfers allowed
- Frozen funds segregated in our accounting systems for traceability
- Assets remain frozen until regulatory authorities provide guidance on resolution

We apply the Process for Freezing of Resources as outlined in Curaçao legal requirements.

7.5 Payment Partner Coordination

Our payment providers (EMIs, PSPs, card processors, crypto gateways) are required to:

- Maintain their own sanctions screening programs
- Notify us immediately of any sanctions hits before processing transactions
- Cooperate in investigations and fund freezing when required
- Provide annual sanctions compliance confirmations

We also conduct our own validation of payment-related sanctions risks:

- Bank Identification Number (BIN) location checks for card transactions
- Geographic analysis of payment origins vs. customer location
- Currency flow analysis from high-risk regions

7.6 Prohibited Jurisdictions

We maintain a zero-tolerance policy for customers or transactions from:

- Countries under comprehensive sanctions
- FATF "Call for Action" jurisdictions
- Regions subject to EU or US embargoes

We enforce these restrictions through:

- IP geolocation blocking at our website level
- VPN and proxy detection systems
- Payment method origin validation
- Document issuing authority verification

Any attempts to circumvent these restrictions are escalated through ICRs and evaluated for STR filing.

7.7 Oversight and Quality Control

- All sanctions screening results logged in our central compliance system

- Compliance Officer reviews all confirmed and potential matches
- Quarterly sanctions compliance reports to CEO and legal counsel
- Annual external audit includes sanctions program effectiveness review
- All staff receive mandatory sanctions compliance training with annual updates

Operational Considerations

Response Times:

- Automatic freezing occurs within minutes of system detection
- Manual review of potential matches completed within 24 hours
- Regulatory notifications filed within 48 hours of confirmed matches

False Positives:

- Common names may generate false positive matches
- We maintain records of cleared false positives to improve future screening efficiency
- Customers affected by false positives have restrictions lifted immediately after verification

System Reliability:

- Our third-party screening system provides 99.9% uptime
- Backup manual screening procedures available if primary system fails
- Regular testing of screening system accuracy and coverage

8. Ongoing Monitoring & Escalation Procedures

Customer verification at onboarding is just the beginning. We maintain ongoing monitoring to detect changes in risk levels, unusual activity patterns, and potential suspicious behavior throughout the customer relationship.

Our monitoring combines automated transaction alerts with manual review processes, designed to catch problems before they become serious compliance issues.

8.1 What We're Trying to Achieve

Our ongoing monitoring aims to:

1. Spot changes in customer risk profiles over time
2. Identify potentially suspicious transactions or behavior patterns
3. Ensure customer information stays current and accurate
4. Assess whether customer activity matches their stated profile
5. Enable timely escalation and reporting when we see red flags

8.2 What We Monitor

Identity and Profile Changes

- KYC document expiration tracking
- Name consistency between documents and payment methods
- Changes in declared occupation, address, or nationality
- Account logins from new countries or unusual locations

Alert Triggers:

- New or updated identity documents
- Payment method names that don't match account holder
- Logins from countries different from stated residence
- Document expiration dates approaching

Transaction Patterns

- Deposit and withdrawal amounts, frequency, and timing
- Ratio analysis (how much they deposit vs. play, win vs. withdraw)
- Use of higher-risk payment methods (crypto, prepaid cards)
- Large transactions that don't fit their declared income or previous patterns

Alert Triggers:

- Multiple deposits just under our €2,200 threshold (potential structuring)
- Multiple prepaid cards or different crypto addresses
- Withdrawals with minimal gameplay
- Detection of third-party payment instruments

Gaming Behavior

- Betting patterns that don't match their stated profile (casual vs. professional gambling)
- Automated or bot-like gameplay patterns
- Unusual win/loss patterns or immediate cash-outs
- Gaming activity timing and location inconsistencies

Alert Triggers:

- 24/7 gaming with very consistent patterns (possible bot activity)
- Repeated bonus abuse attempts
- VPN usage during gameplay but not during deposits/withdrawals

Account Relationships

- Shared IP addresses, devices, or payment methods between accounts
- Affiliate referral patterns suggesting coordinated activity

- Attempts to circumvent our closed-loop payment policy

Alert Triggers:

- Same bank account used across multiple customer accounts
- Affiliate promotions advertising ways to avoid KYC
- Groups of accounts with synchronized activity patterns

Real-Time Transaction Monitoring Rules

Ethoca Integration (Card Fraud Prevention):

- Pre-authorization checks on all card transactions
- Automatic decline for cards reported compromised
- Velocity rules: Max 3 cards per account per 30 days
- BIN country vs IP country mismatch = manual review
- Premium/Business cards = enhanced monitoring

Elliptic/Chainalysis Integration (Crypto Monitoring):

- Real-time wallet screening before deposit acceptance
- Risk scores: 0-100 (auto-reject above 75)
- Mixing service detection = immediate freeze
- Sanctions hit = immediate freeze + legal notification
- Dark web association = EDD trigger

Custom Monitoring Rules (Built in-house):

- RULE_001: Deposit €2,000+ within 60 minutes of registration = Manual Review
- RULE_002: Win/Withdraw ratio >90% with <5% game play = Suspend + Investigation
- RULE_003: 5+ payment methods in 7 days = EDD Trigger
- RULE_004: Structuring: 3+ deposits of €1,900-€2,100 = STR Review
- RULE_005: Dormant account (6 months) sudden €10k+ deposit = Freeze + Review

Slack Alert Channels

#aml-critical (24/7 monitoring):

- Sanctions hits
- PEP matches
- Transactions >€5,000
- Law enforcement requests

#aml-high-priority (business hours):

- Manual review queue >50 items
- System integration failures
- Unusual pattern alerts
- License-specific issues

#aml-daily-review (end of day):

- Failed KYC summary
- Override decisions
- STR filing confirmations
- System performance metrics

Cross-Department Coordination Issues

Common Conflicts:

- VIP Management wants to override limits for high-value players
- Marketing runs promotions that trigger our monitoring rules
- Customer Service promises document reviews "within hours" without checking queue
- Payment team adds new provider without AML review

Resolution Process:

1. All exceptions must be approved in writing via Slack
2. Compliance Officer has veto power on all risk decisions
3. Weekly meeting to review conflicts and update procedures
4. Quarterly training to align departments on AML priorities

8.3 How Our Monitoring Works

Automated Systems

- Transaction monitoring software flags unusual patterns based on predefined rules
- Risk scoring algorithms recalculate customer risk after significant transactions
- Automated alerts for activities exceeding set thresholds (e.g., >€5,000/month, >€1,000 withdrawal without gameplay)
- Event-driven screening when customers add new payment methods or change personal information

Manual Review Process

- Compliance analysts review flagged accounts, gameplay logs, and transaction histories
- Reviews are prioritized based on risk scores, customer geography, transaction amounts, and available intelligence
- Manual reviews are always required for:
 - All Enhanced Due Diligence (EDD) cases
 - Any customer escalated through Internal Concern Reports (ICRs)

- Accounts frozen due to sanctions, PEP matches, or screening hits

8.4 Internal Concern Reports (ICRs)

ICRs are our primary internal escalation mechanism for flagging suspicious activity.

When to File an ICR

- Confirmed or likely sanctions/PEP matches
- Repeated failed verification attempts or refusal to provide required documents
- Refusal to provide source of funds information when requested
- Use of multiple payment methods or suspected third-party funds
- Gaming patterns linked to fraud, bonus abuse, or unusual money movement
- Customer communications suggesting criminal intent or third-party control
- Any activity matching our internal money laundering red flag indicators

ICR Process

1. **Initial alert** from automated systems, customer service, risk team, or payments department
2. **ICR form completion** in our secure compliance system with all relevant details
3. **Compliance Officer review** and priority assignment
4. **Account action decision:**
 - Continue monitoring with enhanced oversight
 - Temporary account suspension pending investigation
 - Account freezing pending STR filing or additional documentation
5. **Documentation and tracking** with timestamps, sources, decision rationale, and resolution status
6. **Final resolution:**
 - Cleared with justification documented
 - Action taken (KYC update, deposit limits, account restrictions)
 - Escalated to Suspicious Transaction Report (STR)

All ICRs are retained for at least 5 years and available for regulatory or audit review.

8.5 Suspicious Transaction Reports (STRs)

When an ICR investigation suggests money laundering or terrorist financing may be occurring, the Compliance Officer must file an STR with the appropriate authorities.

STR Filing Requirements

Curaçao operations: File with FIU Curaçao under NORUT requirements **Estonian operations:** File with FIU Estonia under Estonian AML Act requirements

STR Process

- STRs filed as soon as we have reasonable grounds for suspicion
- Reports completed using required national reporting platforms (goAML or equivalent)

- Supporting documentation compiled (KYC records, transaction history, communications, behavioral analysis)
- STR copy and filing confirmation logged in our internal STR register
- Follow-up actions monitored and recorded (FIU acknowledgment, requests for additional information, investigation outcomes)

Important: Staff are trained never to "tip off" customers about STR filings or ongoing investigations. Disclosing STR information to affected customers is strictly prohibited.

8.6 Documentation and Oversight

- All monitoring actions are logged with timestamps and clear audit trails
- Quarterly reports on ICRs, escalations, and STRs submitted to CEO and archived
- External auditors and regulators have full access to escalation records and decisions
- Periodic review of closed ICRs to ensure consistent decision-making
- Monitoring rules and thresholds reviewed every six months to account for:
 - New money laundering patterns and typologies
 - Regulatory updates and guidance
 - Changes in our business model or customer base
 - Technology improvements and system capabilities

Operational Realities

Processing Times:

- Automated alerts reviewed within 24-48 hours during business days
- ICR investigations typically take 3-10 business days depending on complexity
- STR preparation and filing completed within 5 business days of decision

Resource Constraints:

- Complex investigations may take longer during busy periods or when external verification is required
- Some monitoring may be delayed during system maintenance or upgrades
- Staff availability can affect review timelines, especially during holiday periods

System Limitations:

- Our monitoring systems may not catch every suspicious pattern, particularly sophisticated schemes
- False positives are common and require manual review to clear
- Cross-system data integration occasionally requires manual reconciliation

This monitoring framework ensures we meet regulatory requirements while maintaining practical, sustainable operations across both our Curaçao and Estonian regulatory obligations.

9. Recordkeeping, Retention, and Audit Readiness

Maintaining proper records is essential for demonstrating compliance and supporting regulatory inspections. As a dual-jurisdiction operator, we need to meet recordkeeping requirements for both Curaçao and Estonian regulations, plus EU standards.

Our approach focuses on keeping records organized, accessible, and secure while managing storage costs and data protection obligations.

9.1 What Records We Keep

We maintain the following types of compliance records:

Record Category	What's Included
Customer Identity	ID documents, address verification, biometric verification logs, PEP/sanctions screening results
Address Verification	Utility bills, bank statements, open banking confirmations, address verification service results
Source of Funds/Wealth	Income documentation, bank statements, employment verification, asset sale records, inheritance documents
Transaction Data	Deposits, withdrawals, payment method details, IP addresses, device fingerprints, session logs
Gaming Activity	Bet histories, session timestamps, win/loss records, gameplay patterns, bonus usage
Communications	Customer service chats, emails, compliance correspondence, account restriction notifications
Monitoring Records	Risk scores, alerts generated, investigation notes, system audit trails
Internal Escalations	All ICRs, case files, review decisions, management approvals
Regulatory Reports	STR filings, regulatory correspondence, inspection responses, filing confirmations

Training Documentation	Course completions, test results, attendance records, policy acknowledgments
Audit Materials	Internal audit reports, external audit findings, remediation plans, management responses

9.2 How Long We Keep Records

We follow the stricter requirements between Curaçao and Estonian law:

Record Type	Retention Period	Notes
Customer KYC/CDD	5 years after relationship ends	From last transaction or account closure
Transaction Records	5 years from transaction date	All deposits, withdrawals, bets
ICR/EDD Files	5 years from case closure	Including all supporting documentation
STR Records	5 years from filing date	Plus any follow-up correspondence
Training Records	5 years from completion	Individual completion certificates
Audit Reports	6 years from report date	Internal and external audit materials
Sanctions/Frozen Funds	7 years after resolution	As required by sanctions law

End-of-Life Data Handling

When retention periods expire:

- **Archive:** Low-priority records moved to secure long-term storage with restricted access
- **Delete:** Records destroyed using GDPR-compliant deletion procedures
- **Extended retention:** Records kept longer if ongoing investigations, legal proceedings, or regulatory matters require it

9.3 Storage Systems and Security

Technical Infrastructure

- Daily encrypted backups with offsite storage
- Role-based access controls managed by Compliance Officer and IT Security
- Activity logging for all document access, changes, or downloads
- Multiple secure storage locations (cloud primary, offline backup)
- Version control for policy documents and case files

Access Controls

- **Compliance Officer:** Full access to all records
- **Legal Counsel:** Access to relevant legal and regulatory materials
- **Senior Management:** Access to audit reports and summary materials
- **Audit Teams:** Temporary access during audits with NDA requirements
- **Regulators:** Access provided upon formal request

Data Integrity

- Immutable audit logs for all compliance activities
- Timestamps on all records and system entries
- Change tracking for document uploads and case file updates
- Regular integrity checks and backup testing

9.4 Audit Preparation

We maintain audit readiness for:

- Curaçao Gaming Control Board (CGB) inspections
- FIU Curaçao and Estonian FIU reviews
- Internal and external AML audits
- Banking partner due diligence reviews
- Law enforcement requests

Our Audit Readiness Process

Centralized Document Repository:

- All compliance-critical records stored in searchable database
- Cross-referenced indexing system linking related documents
- Standard templates for common regulatory requests

Response Procedures:

- Compliance Officer designated as primary contact for all audit requests
- Standard 24-48 hour response time for document production

- Pre-prepared document packages for common audit scenarios
- Escalation procedures for urgent law enforcement requests

Quality Assurance:

- Quarterly internal spot-checks of sample records
- Annual completeness review of major case files
- Regular testing of document retrieval systems
- Staff training on audit support procedures

9.5 Data Protection and Privacy

GDPR Compliance

All recordkeeping follows EU General Data Protection Regulation requirements:

- Records used only for AML/CFT compliance purposes
- No reuse of personal data for marketing or commercial analysis
- Proper consent documentation for data processing
- Clear data subject rights procedures

Information Sharing

We only share compliance records with:

- Regulatory authorities (CGB, FIU Curaçao, FIU Estonia)
- Law enforcement agencies with proper authorization
- External auditors under signed confidentiality agreements
- Banking partners for specific due diligence purposes

Staff Training and Confidentiality

All staff with access to compliance records receive training on:

- Confidentiality obligations and data protection requirements
- Internal whistleblowing procedures for reporting data misuse
- Prohibition against unauthorized disclosure or personal use of customer information

Data breaches involving compliance records are treated as major incidents with immediate Board escalation and potential data protection authority notification.

Practical Considerations

Storage Costs

- Active records stored on primary systems for quick access
- Older records moved to lower-cost archive storage
- Regular review of storage needs to manage costs
- Automatic deletion processes for expired records

System Limitations

- Some older records may require manual retrieval during system transitions
- Large file requests may take 24-48 hours to compile
- International data transfer restrictions may affect cross-border audit support
- Backup system testing occasionally requires brief access restrictions

Operational Reality

- Document retrieval times may vary based on record age and format
- Complex multi-year investigations may require additional time to compile complete records
- Some legacy records may have different formatting or quality levels
- Translation services may be needed for documents in multiple languages

This recordkeeping framework ensures we can support regulatory requirements while managing practical operational constraints across our dual-jurisdiction compliance obligations.

10. AML/CTF Governance, Training, and Independent Review

Our AML/CTF program requires ongoing management, staff training, and regular review to stay effective. This section outlines how we organize responsibilities, ensure staff competency, and maintain oversight of our compliance program.

10.1 Organizational Structure

We use a clear governance structure to manage AML/CTF responsibilities across the organization:

Key Roles and Responsibilities

Role	Primary Responsibilities
------	--------------------------

Board of Directors	Approve AML policies and risk appetite; review quarterly compliance reports; sign off on audit findings and required remediation
CEO	Ensure AML is integrated into business strategy and operations; support Compliance Officer with necessary resources; approve compliance budget for tools, training, and audits
Compliance Officer	Manage day-to-day AML program; handle risk assessments and STR filings; update policies; conduct staff training; engage with regulators
Department Heads	Implement AML requirements in their teams; report suspicious activity; support investigations and testing; ensure staff complete required training
All Staff	Complete mandatory AML training; follow CDD/KYC procedures; escalate concerns through proper channels; maintain confidentiality of compliance matters

10.2 Policy Management and Updates

Review Schedule

Our AML policy and procedures are reviewed:

- **Annually** as part of our compliance calendar
- **When regulations change** in Estonia, Curaçao, or EU
- **After significant business changes** (new products, markets, payment methods)
- **Following audit findings** or compliance incidents
- **When regulators provide new guidance** or inspection feedback

Change Management Process

The Compliance Officer maintains a policy version log showing:

- What changed and when
- Who approved the changes (Board approval required for major changes)
- How changes were communicated to staff
- Version control and distribution tracking

Policy updates are distributed through formal notifications, and staff must acknowledge receipt and understanding through our training system.

10.3 Staff Training Program

We provide AML training tailored to different roles and risk levels:

Training by Role

Staff Group	Training Frequency	Focus Areas
New Employees	Before customer contact	AML basics, red flags, escalation procedures
Customer Service & Risk	Annual + updates	Transaction monitoring, identity verification, tipping-off prohibitions
Payments & Finance	Annual	Source of funds validation, cryptocurrency risks, chargeback patterns
Compliance & Legal	Quarterly	Regulatory updates, PEP/sanctions handling, STR procedures
Management & Board	Twice yearly	Strategic AML risks, regulatory developments, audit results
External Contractors	Upon engagement + annual	Basic compliance requirements, prohibited activities

Training Content and Delivery

- **Internal development** for company-specific procedures and systems
- **External providers** for specialized topics (ACAMS, ICA certifications)
- **Online learning platform** with progress tracking and completion certificates
- **Real case studies** from our own experience and industry examples
- **Regulatory updates** covering Curaçao, Estonian, and EU requirements

Training Compliance

- HR and Compliance track completion rates
- Missed training triggers access restrictions and supervisor escalation
- All training records kept for 5 years
- Regular assessment of training effectiveness through testing and feedback

10.4 Employee Screening

For positions involving AML responsibilities, we conduct:

- Criminal background checks focusing on financial crime
- Employment history verification
- Identity document verification
- Reference checks from previous employers
- Review of any relevant AML certifications or experience

Applicants with criminal records related to fraud, money laundering, or financial crime are not eligible for compliance-related roles.

10.5 Internal Auditing and Testing

Internal Audit Program

We conduct internal AML audits at least annually, performed by staff independent from day-to-day compliance operations.

Audit Scope Includes:

- Transaction monitoring system effectiveness
- Accuracy of STR and ICR handling
- Completeness and timeliness of documentation
- Compliance with our risk assessment and policy requirements
- Identification of gaps in controls or procedures

Audit reports go to senior management and the Board, with remediation action plans tracked to completion.

External Audit

Every two years (or more frequently if required by regulators), we engage external AML specialists to review our program.

External audits provide:

- Independent assessment of program effectiveness
- Benchmarking against industry best practices
- Deep-dive review of high-risk areas (cryptocurrency, affiliate traffic, sanctions compliance)
- Regulatory perspective on compliance adequacy

Audit summaries are shared with:

- Curaçao Gaming Control Board during inspections
- FIU Estonia upon request

- Banking and payment partners for due diligence purposes

Performance Metrics

We track key performance indicators including:

- Number and quality of STRs and ICRs filed
- Average time to resolve compliance alerts
- Staff training completion rates and test scores
- Policy update frequency and implementation speed
- Audit finding closure rates

10.6 Management Reporting

The Compliance Officer provides regular reports to management:

Monthly Reports:

- Summary of internal escalations and sanctions/PEP matches
- Monitoring system alerts and resolution status
- Significant compliance issues or regulatory correspondence

Quarterly Reports:

- STR filing activity and regulatory interactions
- Staff training completion statistics
- Upcoming regulatory changes and their impact
- Resource needs and budget considerations

Annual Reports:

- Comprehensive AML program review including audit results
- Business Risk Assessment findings and updates
- Policy changes implemented during the year
- Assessment of program effectiveness and resource adequacy

All reports follow standard templates and are archived for regulatory inspection.

Practical Considerations

Resource Constraints

- Training schedules may need adjustment during busy operational periods
- External audit timing coordinated with business cycles and regulatory calendars
- Budget planning includes provision for regulatory changes requiring additional training or system updates

Dual-Jurisdiction Complexity

- Training materials cover requirements from both Curaçao and Estonian regulations
- Some staff may need specialized training on cross-jurisdictional issues
- Regulatory reporting includes coordination between different FIU requirements

System Dependencies

- Training system integration with HR systems for tracking and compliance
- Audit findings tracked through compliance management system
- Regular backup and testing of training records and completion data

This governance framework ensures our AML program remains effective and current while managing practical operational requirements across our dual regulatory environment.

11. Cooperation with Authorities and Inter-Agency Communication

Operating in multiple jurisdictions means we work with various regulatory and law enforcement authorities. We maintain cooperative relationships with regulators in both Curaçao and Estonia, plus EU-level authorities when required.

Our approach focuses on transparent, timely responses while protecting customer privacy and following proper legal procedures.

11.1 Legal Framework for Cooperation

Our cooperation obligations come from:

- National Ordinance on Reporting Unusual Transactions (NORUT) - Curaçao
- National Ordinance on Identification when Rendering Services (NOIS) - Curaçao
- International Sanctions Act - Estonia
- EU AML Directives and Estonian AML legislation
- FATF Recommendations on international cooperation
- Licensing conditions from the Curaçao Gaming Control Board (CGB)

11.2 Financial Intelligence Units (FIUs)

We maintain regular communication with FIUs in both jurisdictions:

FIU Curaçao

- **STR reporting:** Through designated goAML platform
- **Follow-up requests:** Secure email or formal correspondence

- **Information sharing:** Transaction data, customer profiles, behavioral analysis when requested

FIU Estonia

- **STR reporting:** Through Estonian national reporting system
- **EU coordination:** Compliance with cross-border information sharing requirements
- **Regulatory updates:** Ongoing communication about new requirements and guidance

Types of Cooperation

Suspicious Transaction Reports: Filed immediately when we identify potential money laundering or terrorist financing

Follow-up Information: FIUs may request additional details about filed STRs, including:

- Extended transaction histories
- Customer communication records
- Gaming behavior analysis
- Related account information

Bulk Data Reviews: Occasional requests to review specific customer segments during FIU investigations

Sanctions Coordination: Assistance with asset freezing/unfreezing and blocked account inquiries

All FIU communications are logged, timestamped, and retained for at least 5 years. We request written confirmation of case closure when possible.

11.3 Curaçao Gaming Control Board (CGB)

The CGB serves as our primary AML supervisor for Curaçao operations.

Regular Cooperation

- **License applications:** AML documentation and policy submissions
- **Business Risk Assessments:** Annual BRA reports and control updates
- **Compliance inspections:** Full access to AML programs, training records, STR registers, and monitoring systems
- **Staff interviews:** Cooperation with CGB requests for employee interviews and system demonstrations
- **Documentation requests:** Providing records and analysis as requested

Response Standards

We respond to CGB requests within:

- **2 business days** for routine document requests
- **Immediately** for urgent sanctions or criminal matters
- **5 business days** for comprehensive audits (unless extension pre-approved)

All CGB interactions are logged and stored by the Compliance Officer for audit trail purposes.

11.4 Law Enforcement Cooperation

We may be required to cooperate with criminal investigations through:

- Local police and prosecutor's offices
- Cross-border investigations (Europol, international task forces)
- Mutual Legal Assistance Treaties (MLATs)
- European Investigation Orders

Safeguards and Procedures

All law enforcement requests must be:

- **Written and authorized** (court order, prosecutor authorization, or clear legal basis)
- **Clearly scoped** with specific information requirements
- **Reviewed by legal counsel** before any cross-border data release

We protect confidentiality of unrelated customer information in all disclosures.

The Compliance Officer serves as the single point of contact for law enforcement coordination.

11.5 Sanctions Authority Coordination

When we identify confirmed or suspected sanctions violations:

Immediate Reporting

Curaçao: Sanctions Bureau under Kingdom Sanctions Act

Estonia: Estonian Sanctions Authority

Ongoing Coordination

- Asset freezing and unfreezing procedures
- Transaction tracing for blocked payments
- Beneficiary and originator identification

- Payment flow analysis and documentation

Record Keeping

We maintain detailed logs of:

- All communications with sanctions authorities
- Reference numbers and case tracking
- Resolution status (confirmed violation, false positive, ongoing investigation)

For potential US OFAC or UK OFSI matters, we consult legal counsel before filing voluntary disclosures.

11.6 Data Protection in External Cooperation

All information sharing follows:

- **GDPR requirements** for EU/Estonian operations
- **Curaçao data protection principles**
- **Purpose limitation:** Data shared only for AML/CTF purposes
- **Detailed logging:** Every external disclosure documented with date, recipient, legal basis, and approval

Disclosure Documentation

Our external disclosure log includes:

- Date and time of request and response
- Identity of requesting authority
- Specific data or documents provided
- Legal authorization or basis for disclosure
- Compliance Officer or legal counsel sign-off

Staff are prohibited from sharing AML-related information with unauthorized parties. All disclosures must follow our internal procedures with proper documentation.

11.7 Staff Training on Authority Cooperation

Relevant staff receive training on:

- **Immediate escalation:** All regulator and law enforcement contact goes directly to Compliance Officer or Legal team
- **Tipping-off prevention:** Never disclose STRs or ongoing investigations to customers
- **Information protection:** Maintaining confidentiality and integrity of shared data
- **Proper procedures:** Following formal request and approval processes

Training includes practical scenarios and case studies to help staff recognize and properly handle authority interactions.

Operational Realities

Response Challenges

- **Language barriers:** Some requests may require translation services
- **System limitations:** Older records may take longer to retrieve and compile
- **Resource constraints:** Complex requests during busy periods may require deadline extensions
- **Cross-jurisdiction complexity:** Coordinating between different legal frameworks and requirements

Communication Management

- **Primary contact:** Compliance Officer handles all formal authority communications
- **Backup procedures:** Legal counsel available for complex or urgent matters
- **Documentation standards:** All interactions documented regardless of formality
- **Follow-up tracking:** Monitoring status of ongoing requests and investigations

Practical Considerations

- International time zone differences may affect response timing
- Some authorities prefer specific communication channels or formats
- Relationship management helps ensure smooth cooperation during investigations
- Regular training keeps staff current on proper escalation and communication procedures

This cooperation framework ensures we maintain positive working relationships with all relevant authorities while meeting our legal obligations across both licensing jurisdictions.

12. Breach Consequences and Enforcement Mechanisms

We take AML policy violations seriously and have clear consequences for non-compliance. This section outlines what happens when someone fails to follow our AML procedures, whether intentionally or through negligence.

Our approach is proportionate - minor oversights are treated differently than serious violations - but we maintain consistent enforcement to ensure everyone understands the importance of compliance.

12.1 Who This Applies To

This enforcement policy covers:

- All employees (full-time, part-time, temporary)
- Management and executives
- Contractors and consultants working with customer data
- Third-party service providers with AML obligations (KYC vendors, payment processors)

We distinguish between intentional misconduct and honest mistakes, but both can result in consequences depending on the severity and impact.

12.2 Types of Violations

Procedural Violations

- Failing to complete required Customer Due Diligence (CDD) or Enhanced Due Diligence (EDD)
- Ignoring or not escalating red flags or suspicious activity
- Not filing Internal Concern Reports (ICRs) or Suspicious Transaction Reports (STRs) when required
- Falsifying or manipulating customer information
- Bypassing or disabling transaction monitoring systems

Disclosure Violations

- **Tipping off** customers about ongoing investigations or STR filings
- Sharing AML-related information with unauthorized people
- Discussing compliance matters outside proper channels

Negligence and Omissions

- Incomplete customer verification or documentation
- Failing to screen customers for sanctions or PEP status when required
- Missing regulatory filing deadlines
- Ignoring document expiration dates or high-risk account flags

Management Failures

- Not implementing AML policies in their department
- Reducing compliance resources without proper justification
- Hiding audit findings or failing to implement required improvements

12.3 Consequences and Disciplinary Actions

We use a graduated approach based on severity and intent:

Severity Level	Examples	Typical Actions
Minor (Negligent)	Forgetting to upload a document; minor oversight on low-risk account	Verbal warning + additional training
Moderate	Failing to escalate suspicious activity; repeated documentation errors	Written reprimand; temporary restrictions; closer supervision
Serious	Knowingly ignoring sanctions match; falsifying CDD information; pattern of violations	Final warning; possible termination; regulatory notification if required
Severe/Criminal	Tipping off customers; fraud; collusion; deliberate concealment	Immediate termination; law enforcement referral; legal action

Documentation and Tracking

All disciplinary actions are:

- Recorded in HR and compliance systems
- Tracked for patterns of repeat behavior
- Escalated to legal counsel when appropriate
- Reported to authorities if criminal activity is suspected

12.4 Third-Party Violations

Vendors and service providers with AML obligations (payment processors, KYC providers, customer service outsourcers) face:

- Service suspension or contract termination
- Notification to relevant licensing authorities
- Legal action for damages caused by violations
- Inclusion on our internal "restricted vendor" list

The Compliance Officer documents all third-party violations and coordinates with Legal, Procurement, and senior management on appropriate responses.

12.5 Self-Reporting and Whistleblowing

We encourage staff to report their own mistakes and violations by others:

Self-Reporting Benefits

- Employees who self-report unintentional violations won't face termination for first-time offenses (unless involving gross negligence or criminal intent)
- Self-reporting is considered a mitigating factor in disciplinary decisions
- We focus on fixing problems rather than punishment when staff proactively identify issues

Whistleblower Protection

- Confidential reporting channel available for staff to report violations by colleagues
- Strict prohibition against retaliation - retaliating against whistleblowers is grounds for immediate termination
- Anonymous reporting options available when appropriate
- All whistleblower reports investigated by Compliance Officer with HR and Legal oversight

12.6 Remediation and Improvement

After any significant violation, we implement structured remediation:

Root Cause Analysis

- Determine if the problem was due to individual error, inadequate procedures, or system failures
- Identify whether additional training, policy changes, or system improvements are needed
- Review whether similar problems exist elsewhere in the organization

Corrective Actions

- **Process improvements:** Better controls, enhanced monitoring, mandatory approvals
- **Training updates:** Additional training for affected individuals or departments
- **System changes:** Technical fixes to prevent similar problems
- **Policy clarification:** Updates to procedures or guidance documents

Follow-up and Monitoring

- Internal audit review within 3-6 months to ensure fixes are working
- Ongoing monitoring of affected areas for improvement
- Regular reporting to management on remediation progress

12.7 Regulatory Reporting

We report violations to authorities when they:

- Involve potential criminal activity
- Could affect our licensing status
- Represent material failures in our AML controls
- Put customer funds, data, or regulatory compliance at risk

Reporting Process

Authorities we may notify:

- Curaçao Gaming Control Board (CGB)
- FIU Curaçao or FIU Estonia (depending on jurisdiction)
- Sanctions authorities (if involving frozen assets or sanctioned persons)
- Affected financial institutions or payment partners

Reporting coordination:

- Compliance Officer leads all regulatory notifications
- Legal counsel reviews all external communications
- External disclosures logged in our disclosure register
- CEO or Board member sign-off required for significant reports

This ensures we maintain regulatory trust and meet our legal obligations while responding appropriately to compliance failures.

Practical Considerations

Investigation Timelines

- Minor violations: Resolved within 1-2 weeks
- Moderate violations: 2-4 weeks including remediation planning
- Serious violations: 4-8 weeks with potential legal and regulatory involvement
- Criminal matters: Timeline determined by law enforcement requirements

Resource Impact

- Investigations may require temporary reassignment of staff
- External legal counsel may be needed for complex cases
- Some violations may require immediate system changes or additional controls
- Training updates and policy revisions take time to implement and communicate

Documentation Requirements

- All violation investigations documented regardless of outcome

- Evidence preservation for potential regulatory or legal proceedings
- Regular review of violation patterns to identify systemic issues
- Anonymous trend reporting to senior management and Board

Our enforcement approach balances the need for accountability with recognition that mistakes happen, while ensuring serious violations receive appropriate consequences.

13. Use of Physical Establishments and White-Label Gaming Models

MoonRocket does **not currently operate any physical gambling establishments**, retail kiosks, or white-label partner platforms. All customer interactions occur exclusively through our proprietary digital platform, and all account access, verification, and transactions are performed online.

However, should MoonRocket decide to expand into **kiosk-based, agent-based, or white-label business models** in the future, we commit to the following regulatory and AML/CFT safeguards in line with Curaçao GCB Regulations (January 2025), Section III.15:

13.1 Pre-Launch Due Diligence on Physical/Partner Operators

Before onboarding any kiosk operator, white-label partner, or retail facilitator, MoonRocket will:

- Conduct full **corporate due diligence**, including:
 - UBO identification and verification
 - AML history and licensing status
 - Criminal background screening of directors and controllers
- Require a **signed AML attestation** that partner staff have received and will apply our AML/CFT policy.
- Perform an **on-site audit** (if applicable) to evaluate infrastructure, customer touchpoints, and operational risks.

13.2 Mandated Use of MoonRocket AML Systems and KYC Tools

All physical or white-label points of customer onboarding will be required to:

- Use MoonRocket's central **KYC identity verification system**, including biometric liveness checks.
- Submit customer identity data in real-time through our onboarding API.
- Disable account creation, cash-in/cash-out, or registration unless verification is completed successfully.

- Follow the same **risk-scoring, sanctions, and PEP screening processes** as direct platform users.

13.3 Transaction Monitoring and Compliance Oversight

- All transactions facilitated through partners must pass through MoonRocket's centralized **transaction monitoring system**, including SEON risk scoring, payment profiling, and rule-based alerts.
- Suspicious activity detected through third-party channels will trigger **Immediate Internal Concern Reports (ICRs)** and may result in:
 - Withdrawal freeze
 - Partner suspension
 - STR filing with the FIU

13.4 Staff Training and Certification

Any partner staff interacting with customers must complete:

- AML/CFT training certified by MoonRocket Compliance within 30 days of onboarding
- Annual refreshers on AML procedures, tipping-off risks, and sanctions escalation
- A test or assessment confirming understanding of KYC and red-flag behavior

Training logs will be stored and audited annually.

13.5 Mandatory Pre-Notification to the GCB

Prior to launch of any such physical or white-label model, MoonRocket will:

- Notify the Curaçao Gaming Control Board in writing at least **30 days in advance**
- Submit:
 - An updated Business Risk Assessment (BRA)
 - Detailed partner onboarding procedures
 - A demonstration of how KYC/AML will be controlled across partner channels
- Seek written confirmation or guidance from the GCB before launch

13.6 Termination of Non-Compliant Partners

If any physical outlet, kiosk, or white-label partner fails to adhere to our AML/CFT framework, MoonRocket reserves the right to:

- **Immediately suspend all access** to the platform and block accounts created via the offending channel
- **Terminate the commercial relationship** pending review
- Notify the FIU and the GCB if serious or repeated breaches occur

14. Document Control, Ownership, and Certification

This section covers how we manage this AML policy document itself - who's responsible for it, how we handle updates, and the approval process for changes.

14.1 Document Information

Field	Details
Policy Title	MoonRocket Anti-Money Laundering and Counter-Terrorist Financing Policy
Scope	All entities under MoonRocket Holdings, including MagicPoro Ltd (CY) and EastPoint Operations B.V.
Document Owner	Compliance Officer
Approval Authority	Board of Directors / UBO
Current Version	1.5 (Updated for CGB regulatory alignment and practical implementation)
Effective Date	30.05.2025
Review Schedule	Annual review, or when regulatory changes require updates
Next Review Due	1.05.2026
Storage Location	Compliance system (restricted access), internal policy portal, regulatory submission files

14.2 Approval Process

This policy was:

- **Developed by:** Compliance Officer with input from Legal and Operations teams
- **Reviewed by:** Legal Counsel and senior management
- **Approved by:** Board of Directors/UBO on 30.05.2025

Once approved, this policy:

- Gets distributed to all department heads and managers
- Is made available to all staff through our internal policy portal
- Becomes mandatory for all operations and serves as the basis for compliance training
- May result in disciplinary action for non-compliance as outlined in Section 12

14.3 Change Management

When Updates Are Needed

We update this policy when:

- Annual review identifies areas for improvement
- Regulatory changes in Curaçao, Estonia, or EU require policy adjustments
- New business activities or products create additional AML risks
- Internal audits or regulatory inspections identify gaps
- Significant compliance incidents require policy clarification

Update Process

All policy changes follow a formal process:

1. **Change proposal** by Compliance Officer with business justification
2. **Review** by Legal counsel and relevant department heads
3. **Approval** by CEO for minor changes, Board of Directors/UBO for major revisions
4. **Version control** with clear documentation of what changed and why
5. **Staff communication** through formal notifications and training updates

Version History

Version	Date	Summary of Changes	Approved By
1.0	June 2022	Initial AML policy	UBO / Compliance officer

1.1	March 2023	General update of different sections	UBO / Compliance officer
1.3	Feb 2024	Updated for CGB regulatory alignment	UBO / Compliance officer
1.4	May 2024	Updated for EMTA / EU regulatory alignment	UBO / Compliance officer
1.5	May 2025	Updated for CGB regulatory alignment, practical implementation considerations, and operational clarity	UBO / Compliance officer

No staff member or department can modify this policy or create local exceptions without written approval from the Compliance Officer and CEO.

14.4 Management Certification

By approving this policy, our senior management certifies that:

- We have implemented an AML/CTF framework that meets our regulatory obligations in both Curaçao and Estonia
- Adequate resources, staff, and systems are allocated to execute the controls outlined in this policy
- This policy has been reviewed and understood by the Compliance Officer and relevant senior management
- We commit to regular review and updates to maintain effectiveness and regulatory compliance

14.5 Signature Page

For MoonRocket Holdings Ltd:

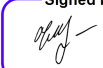
Director

Signed by:
Signature: 
B19EE4607B28455...

Name: Igor Patlan

Date: 30.05.2025

Compliance Officer

Signed by:
Signature: 
C7318F93CC684F5...

Name: Olena Chaplytska

Date: 30.05.2025

Ultimate Beneficial Owner

DocuSigned by:
Signature: 
5C0F0E709DDA4FE...

Name: Nicola Magro

Date: 30.05.2025