

Anti-Money Laundering (AML) & Counter-Terrorism Financing (CTF) Policy

ClubR10 – Operated by Zerone B. V.
Version 1.0

1. Introduction

This Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) Policy applies to ClubR10, a brand operated by Zerone B. V., licensed and regulated by the Curaçao Gaming Authority (CGA).

Its purpose is to prevent the use of the platform for money laundering, terrorist financing, illicit fund movements, or any other financial crimes. The policy establishes mandatory procedures for customer assessment, transaction monitoring, analysis of suspicious activities, and proper escalation.

All monitoring and investigations under this policy are performed manually by trained Compliance, Fraud, Risk & Payments personnel.

2. Purpose of the AML Policy

The objectives of this AML/CTF Policy are to:

1. Prevent and detect money laundering, terrorist financing, and the concealment of illicit funds.
 2. Ensure full compliance with Curaçao's gaming regulations and international AML standards.
 3. Establish clear internal responsibilities across operational teams.
 4. Maintain systematic monitoring of customer activity and transactional behavior.
 5. Provide a structured framework for reporting, escalation, and record keeping.
 6. Protect the integrity, security, and trustworthiness of the ClubR10 platform.
-

3. Scope

This AML Policy applies to:

- All customers using the ClubR10 platform.
- All deposits, withdrawals, bets, transfers, and financial interactions.
- All teams involved in customer verification, payment processing, and risk monitoring.

- All manual reviews conducted by Compliance, Fraud, Risk & Payments teams.

The policy is mandatory for every staff member with operational access.

4. Key AML Principles

1. Know Your Customer (KYC)

Customer identity must be verified before any withdrawal, in accordance with the KYC Policy.

2. Customer Due Diligence (CDD)

Documented and consistent processes must be used to confirm customer identity and evaluate risk.

3. Enhanced Due Diligence (EDD)

Additional checks must be performed for high-risk customers or suspicious cases.

4. Transaction Monitoring

All transactional behavior is manually monitored to identify irregular or suspicious activity.

5. Record Keeping

All AML-related actions, reviews, and reports must be stored securely for at least 5 years.

6. Escalation & Reporting

Serious or confirmed suspicious cases must be escalated and may be reported to the CGA.

5. Customer Due Diligence (CDD)

CDD is mandatory for all customers requesting withdrawals.

5.1 Verification Requirements

- Valid ID with photo and CPF
- Proof of address (issued within 6 months)
- Consistency between documents and account details
- Compliance checks on identity and address

5.2 Customer Risk Categorization

Customers are classified as:

- Standard Risk – normal betting patterns and financial activity
- Medium Risk – irregular but not suspicious behavior

- High Risk – unusual, potentially fraudulent, or high-value activity

Risk level is adjusted dynamically based on behavior, documentation, and transaction patterns.

6. Enhanced Due Diligence (EDD)

EDD is required when customer behavior or documentation indicates elevated risk.

EDD triggers include:

- Unusual deposit patterns
- Repeated high-value withdrawals
- Multiple accounts linked by same details
- Use of third-party cards or wallets
- Inconsistent KYC documents
- Suspicion of identity manipulation
- Abnormal betting behavior
- Attempts to bypass verification or limits

EDD measures may include:

- Additional identity documents
 - Proof of payment methods
 - Proof of source of funds (SOF)
 - Account suspension during investigation
 - Manual interview via customer support
 - Escalation to Fraud & Risk
-

7. Ongoing Monitoring & Detection

Monitoring is performed by Compliance and Fraud, Risk & Payments teams.

7.1 Transaction Analysis

Teams manually review:

- Deposit frequency and methods
- Withdrawal patterns and velocity

- Cash-in / cash-out matching behavior
- Rapid deposit–withdraw cycles
- Use of multiple accounts or devices
- Suspicious IP, VPN, or location patterns

7.2 Betting Behavior Monitoring

Indicators include:

- Low-risk betting with guaranteed outcomes
- Arbitrage or hedge patterns
- Betting inconsistent with customer profile
- Round-tripping behavior

8. Suspicious Activity Indicators

Examples of suspicious customer behavior:

- Depositing large amounts and not betting proportionally
- Depositing and immediately requesting withdrawal
- Using multiple payment methods or third-party accounts
- Accounts linked to fraud, chargebacks, or abuse
- Attempts to influence or bypass KYC rules
- Refusal to provide requested information
- Sudden changes in device, IP, or personal data
- Customer statements inconsistent with financial activity

Any of these indicators requires **mandatory internal escalation**.

9. Internal Reporting & Escalation Process

9.1 Internal Escalation Steps

1. Suspicion Identified

CS, Fraud, Risk, or Compliance detects signs of irregularity.

2. Case Documentation

Analyst records evidence, screenshots, history, and transactional data.

3. Internal Review

Fraud & Risk team performs detailed analysis.

4. Decision

- Case cleared
- Customer required to submit more documents
- Account limited or suspended
- Account closed
- Case escalated for regulatory reporting

9.2 Reporting to CGA

If required, serious cases will be:

- Fully documented
- Escalated to legal
- Reported to the Curaçao Gaming Authority (CGA)

The Compliance team is responsible for final evaluation and regulatory communication.

10. Data Storage and Protection

- All AML records are stored for **5 years**.
 - Access is restricted to:
 - Compliance
 - Fraud, Risk & Payments
 - Customer Support (limited operational data)
 - Administrative/management personnel
 - Platform security is maintained by the **third-party platform provider**.
 - All data storage complies with **LGPD** and international privacy laws.
-

11. Internal Roles and Responsibilities

Team / Department	Responsibilities
Compliance / KYC Team	Oversees AML framework, performs due diligence, conducts EDD, validates escalations, approves regulatory reporting.

Team / Department	Responsibilities
Fraud, Risk & Payments	Monitors deposits, withdrawals, betting activity; investigates suspicious cases; escalates to Compliance.
Customer Support (CS)	Frontline detection of unusual behavior, collecting documents, informing customers of AML requirements.
Administrative / Directors	Oversight and approval of high-impact AML decisions.
Third-Party Platform Provider	Ensures platform security, technical infrastructure, and system stability.

12. Training

All staff with access to customer data receive AML/CTF training, including:

- Detecting suspicious behavior
- Following escalation procedures
- Understanding KYC and SOF requirements
- Data protection and confidentiality
- Regulatory obligations under CGA

Training occurs upon onboarding and annually.

13. Record Keeping

The company maintains secure logs of:

- All AML reviews and escalations
- Evidence used in investigations
- Customer documentation
- Communication with customers and regulators

Retention period: **minimum 5 years**.

14. Policy Review & Updates

This AML Policy is reviewed:

- Annually

- After regulatory updates from the CGA
- When changes in operational or risk processes require revisions

Revisions are archived and version-controlled.

A handwritten signature in black ink, consisting of a large, stylized 'Z' followed by a vertical line and a small flourish.

Zerone B.V.

Virae Management B.V. - Director

Represented by Veysel Demir

15 November 2025