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

ClubR10 – Operated by Zerone B. V.
Version 2.0

1. Introduction

ClubR10, operated by Zerone B. V. and licensed by the Curaçao Gaming Authority (CGA), is committed to maintaining the highest standards of integrity and compliance in its operations. This Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) Policy sets out the procedures, responsibilities, and controls designed to prevent the platform from being exploited for illicit financial purposes, including money laundering, terrorist financing, and other unlawful activities.

The policy applies to all customers, financial transactions—including deposits, withdrawals, bets, and transfers—and employees who have access to sensitive financial information. Manual monitoring, investigations, and risk-based assessments are conducted by the Compliance Team in coordination with the Fraud, Risk & Payments Team. Senior management retains ultimate accountability for ensuring that all aspects of AML/CTF compliance are executed effectively.

By implementing this policy, ClubR10 ensures that all operational processes are aligned with regulatory requirements and international best practices, safeguarding both the company and its customers from financial crime risks.

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

2. Purpose

The purpose of this policy is to provide a comprehensive framework for mitigating money laundering and terrorism financing risks within ClubR10's operations. It aims to:

- Establish clear responsibilities and procedures for teams involved in verification, monitoring, and risk assessment
- Ensure consistent, risk-based approaches to customer due diligence and enhanced scrutiny of high-risk cases
- Define structured processes for internal escalation and regulatory reporting
- Maintain secure, auditable records of all AML/CTF activities

- Integrate controls to prevent financing of weapons proliferation and ensure compliance with sanctions

Through these measures, ClubR10 protects the platform's integrity, promotes transparency, and reinforces the trust of both customers and regulatory authorities.

3. Scope

This policy applies comprehensively to all aspects of ClubR10 operations, encompassing:

- Every customer account and transaction on the platform
- Deposits, withdrawals, bets, transfers, and other financial interactions
- Staff involved in verification, monitoring, risk assessment, investigations, and operational support
- Employees with access to sensitive financial information

The scope ensures that AML/CTF controls are applied consistently across all business areas, guaranteeing adherence to CGA and international standards.

4. Governance and Responsibilities

ClubR10 has established a clear governance framework to manage AML/CTF risk. The Compliance Team oversees policy execution and monitors adherence to regulatory requirements, while senior management retains ultimate accountability. All business units collaborate to ensure proper risk management. Responsibilities are distributed as follows:

- **Compliance Team:** Oversees the entire AML/CTF program, validates escalations, approves regulatory reporting, and ensures compliance with CDD/EDD, CPF, and sanctions procedures.
- **Fraud, Risk & Payments Team:** Continuously monitors transactions and betting activity, investigates operational anomalies, and escalates potential AML concerns.
- **Customer Support:** Acts as the frontline, identifying unusual behaviour, collecting documentation, and informing customers of AML/KYC obligations.
- **Senior Management:** Provides oversight of high-impact decisions, ensuring alignment with governance and regulatory standards.

- **Third-Party Platform Provider:** Maintains secure infrastructure, supporting transaction monitoring, data retention, and operational stability.

This governance structure ensures accountability, clarity, and coordination across all departments, enabling effective risk mitigation.

5. Risk Assessments

5.1 Business Risk Assessment (BRA)

ClubR10 conducts an annual BRA to evaluate the company's exposure to financial crime risks. The assessment examines products, services, distribution channels, transaction volumes, and geographic risk factors. It identifies potential vulnerabilities and informs the application of proportionate controls.

- Risk factors include betting types, transaction patterns, high-risk jurisdictions, and the company's regulatory history
- Risks are classified as low, medium, or high, guiding mitigation strategies such as deposit limits and enhanced monitoring
- The Compliance Team ensures documentation is maintained for audits and regulatory inspections

5.2 Customer Risk Assessment (CRA)

The CRA is conducted at onboarding and continuously throughout the customer relationship to evaluate risk factors, including:

- Country of residence and regulatory exposure
- Source and consistency of funds
- Transactional activity and account history
- Sanctions or PEP status

Clients are classified as low, medium, or high risk, which determines the intensity of monitoring and due diligence applied. CRA outcomes are documented and securely maintained for at least five years.

6. Customer Acceptance and Due Diligence

6.1 Customer Acceptance Policy (CAP)

The Customer Acceptance Policy establishes the criteria and conditions under which a customer is allowed to open and maintain an account. It ensures that only customers

whose basic information can be verified—and who do not present immediate high-risk indicators—are permitted onto the platform.

During onboarding, the Company collects essential personal information to support downstream due diligence. Automated screening is performed to prevent onboarding of sanctioned individuals, PEPs from high-risk jurisdictions, or customers with clear signs of impersonation or fraud. The CAP ensures that only customers who can later complete CDD/EDD requirements are accepted, maintaining alignment with the Company's AML/CTF/CPF risk appetite.

Key CAP Requirements:

- Collection of accurate personal information upon registration
- Automated sanctions / PEP / CPF watchlist screening
- Rejection of customers from prohibited or unverified jurisdictions
- Blocking of accounts with inconsistent, incomplete, or fraudulent information
- Compliance review required for customers identified as Medium or High risk before they can proceed with continued activity

6.2 Customer Due Diligence (CDD)

CDD is mandatory for all customers who reach cumulative deposits of **NAf 4,000**, request **any withdrawal**, or present **behavioural or jurisdiction-based risk indicators**. It ensures that customer identity and address are verified, that the risk profile is assessed, and that the platform is not exploited for illicit purposes.

If discrepancies or risk factors are identified, the customer may be escalated to EDD or rejected under the CAP.

CDD Procedures Include:

- Verification of government-issued identification
- Verification of address (PoA)
- Screening against updated sanctions, PEP, adverse media and CPF lists
- Review of customer profile consistency, behaviour, and transaction patterns
- CRA-based assignment of Standard, Medium, or High risk

Customers classified as Medium or High risk are restricted until the Compliance Team completes review and issues approval. Customers failing CDD are rejected according to CAP.

6.3 Enhanced Due Diligence (EDD)

EDD is required when customer behavior or documentation indicates elevated risk as per CRA. Additional triggers include potential PF involvement, sanctions hits, and irregular account patterns.

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. Decision Outcomes (Post-CAP, CDD, CRA, and EDD)

All due diligence processes must lead to a clear decision. The Company ensures decisions are consistent, timely, and appropriately documented to support audit and regulatory oversight.

Possible Outcomes Include:

1. Approved (Standard Risk)

- Customer passes CDD
- No material inconsistencies
- Allowed to continue normal activity

- Subject to routine monitoring

2. Approved with Conditions (Medium Risk)

- Customer presents some risk indicators
- CDD completed but requires periodic follow-up
- Activity may be limited (deposit caps, verification reminders)
- Monitoring frequency increased

3. Approved after EDD (High Risk)

- High-risk customer cleared through EDD
- Requires ongoing enhanced monitoring
- MLRO must review periodically
- Subject to strict deposit/withdrawal controls

4. Pending / Restricted

- Documentation required
- Verification unresolved
- Withdrawal requests frozen until completion
- Account partially limited

5. Rejected or Off-boarded

Customers are rejected under the CAP or closed after review if:

- Documents are forged or unverifiable
- SOF/SOW cannot be validated
- Behaviour suggests ML/TF/PF risk
- They appear on sanctions, PEPs from high-risk jurisdictions, or CPF lists
- They fail or refuse to complete CDD/EDD

All rejections include internal documentation with justification.

8. Transaction Monitoring and Detection

ClubR10 continuously monitors transactions and betting activity to detect unusual behavior indicative of financial crime. Monitoring focuses on patterns such as:

- Frequency and volume of deposits and withdrawals
- Matching deposit and withdrawal behavior (round-tripping)
- Multiple accounts linked to a single customer
- Suspicious IP addresses or VPN usage
- Betting activity inconsistent with the customer's profile, including arbitrage or guaranteed outcomes

Suspicious activity is documented and escalated to the Compliance Team for investigation and potential regulatory reporting.

9. Counter-Proliferation Financing (CPF)

To prevent financing of weapons proliferation, ClubR10 implements procedures to identify, block, and report suspicious activity:

- Customers, transactions, and partners are screened against international proliferation lists
 - Suspicious transactions are immediately blocked and investigated
 - Compliance conducts detailed reviews, reporting confirmed or suspected cases to the relevant authorities
 - Documentation of all actions ensures auditability and regulatory compliance
-

10. Sanctions Screening and Freezing

ClubR10 screens all customers and transactions against applicable sanctions lists. When a match is identified:

- Funds are immediately frozen
- Further transactions are suspended pending review
- Compliance documents all actions and notifies the Curaçao Gaming Authority (CGA)
- Customer status is continuously monitored until resolution

This ensures full compliance with national and international regulatory obligations.

11. Internal Reporting and Escalation Process

11.1 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 | |
| <ul style="list-style-type: none">○ Case cleared○ Customer required to submit more documents○ Account limited or suspended○ Account closed○ Case escalated for regulatory reporting | |

11.2 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.

12. Audit Record-Keeping, and Data Protection:

ClubR10 maintains a rigorous framework for auditing, record-keeping, and data protection, ensuring that all AML/CTF activities are traceable, auditable, and compliant with regulatory obligations. Regular audits and secure documentation are fundamental to maintaining transparency and accountability across the organization.

Audits:

The company conducts **annual independent AML/CFT audits**, which may be performed by internal auditors or external specialists. The audit scope includes:

- Evaluation of the effectiveness of policies and procedures
- Assessment of the quality and completeness of customer due diligence (CDD/EDD)

- Review of transaction monitoring and suspicious activity reporting
- Compliance with sanctions and Counter-Proliferation Financing (CPF) obligations
- Verification of internal escalation processes and operational execution

Audit findings are documented in a formal report, including:

- Identified gaps or weaknesses
- Recommendations for corrective actions
- Assigned responsibilities and implementation timelines
- Follow-up procedures to ensure gaps are addressed

Record-Keeping:

ClubR10 maintains **comprehensive and secure records** of all AML-related activities to ensure regulatory compliance and audit readiness. Records include:

- Business Risk Assessment (BRA) and Customer Risk Assessment (CRA) documentation
- Customer Acceptance Policy (CAP) decisions
- CDD and EDD measures
- Sanctions actions and freezing procedures
- Counter-Proliferation Financing alerts and investigation results
- Internal employee integrity screening outcomes
- Audit reports and follow-up documentation

All records are **retained for a minimum of five years**, with access restricted to authorized personnel, including Compliance, Fraud, Risk & Payments, Customer Support (limited operational data), and senior management.

Data

Protection:

Sensitive data is protected in compliance with **LGPD** and applicable international privacy standards. Measures include:

- Secure storage and encryption of all AML/CTF records
- Role-based access control to limit exposure of sensitive information
- Data processing and retention aligned with regulatory requirements
- Collaboration with the Third-Party Platform Provider to ensure system stability, integrity, and protection against unauthorized access

These practices guarantee that all AML/CTF activities are **fully traceable, auditable, and protected**, enabling ClubR10 to demonstrate compliance to regulators and auditors at any time.

13. Employee Integrity and Training

ClubR10 recognizes that the effectiveness of AML/CTF measures depends heavily on the integrity and competence of its employees. The company implements comprehensive integrity verification and training programs to ensure staff can identify and manage risks effectively.

Employee	Integrity	Verification:
-----------------	------------------	----------------------

All employees undergo **rigorous checks prior to hiring**, which include:

- Criminal background verification
- Professional history and employment reference checks
- Assessment of involvement in prior financial crimes or conflicts of interest

Employees in critical roles, particularly in compliance, risk, and finance, are subject to **periodic re-evaluation** to ensure ongoing compliance with internal standards. Those who fail to meet established integrity criteria are either not hired or have their responsibilities adjusted to mitigate potential AML/CTF exposure.

Training	Program:
-----------------	-----------------

Training is **mandatory at onboarding** and repeated **annually** to maintain awareness and competence. Training content includes:

- Identification of suspicious activities and transaction patterns
- Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) processes
- Awareness of Counter-Proliferation Financing (CPF) risks
- Sanctions compliance and freezing procedures
- Internal reporting, escalation, and documentation requirements
- Data protection, confidentiality, and privacy standards

Objectives of Training:

- Equip employees with the knowledge to detect money laundering and terrorist financing risks
- Ensure correct application of internal AML/CTF procedures
- Reinforce the company's ethical standards and regulatory compliance culture

Training effectiveness is monitored through assessments and periodic refresher courses, ensuring that employees remain vigilant and competent in supporting the AML/CTF framework.

14. Policy Review and Updates

ClubR10 maintains a **dynamic and proactive approach** to AML/CTF compliance through regular review and updates of this policy. This ensures that the company's procedures remain aligned with regulatory changes, industry best practices, and evolving risk environments.

Review Process:

The policy is formally reviewed **at least annually**, and additionally:

- Following regulatory updates or guidance from the Curaçao Gaming Authority (CGA)
- Upon identification of operational changes or emerging risks
- After significant audit findings or internal control assessments

Update

Procedures:

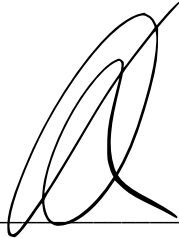
During review, the company examines:

- Business Risk Assessment (BRA) and Customer Risk Assessment (CRA) frameworks
- Customer Acceptance Policy (CAP), CDD, and EDD thresholds
- Transaction monitoring, sanctions, and CPF procedures
- Internal escalation and reporting workflows
- Employee integrity and training programs

Documentation and Version Control:

- All revisions are **documented, archived, and version-controlled**
- Historical records of policy changes are maintained for transparency and accountability
- Updates are communicated to all employees, ensuring full awareness and consistent application

By maintaining a structured review and update cycle, ClubR10 ensures that its AML/CTF policy remains **current, effective, and fully compliant** with regulatory requirements and international standards.



Zerone B.V.

Virae Management B.V. - Managing Director

Represented by V. Demir

11 December 2025