

Anti-Money Laundering Policy

Welcome to the All The Best Lottos (ATBL), Sirr Lotto, and 232casino Anti-Money Laundering and Due Diligence Procedures. This document outlines the procedures followed regarding Anti-Money Laundering (AML), Counter Financing of Terrorism (CFT), and Know Your Customer (KYC) practices. Our procedures below describe how we address AML, CFT & KYC requirements applicable to the Company, and in assisting and reminding all staff members of their obligations and personal responsibility under the legislation of the country of Curacao.

1. Introduction

This Anti-Money Laundering (“AML”) and Counter Financing of Terrorism (“CFT”) Policy (the “Policy”) sets out the framework, procedures, and responsibilities that K.I.K Corporation B.V. (“the Company”) has adopted to comply with its obligations under the laws and regulations of Curaçao.

The purpose of this Policy is to ensure that the Company implements adequate and effective systems to prevent its services and operations from being misused for the purposes of money laundering, terrorist financing, or any other financial crime.

This Policy reflects the requirements of the **National Ordinance on the Prevention and Combating of Money Laundering and Terrorist Financing (NOIS and NORUT)**, the **National Ordinance on Offshore Games of Hazard (LOK)**, and the regulatory guidance issued by the **Curaçao Gaming Control Board (GCB)** and the **Curaçao Gaming Authority (CGA)**, including the updated **GCB AML Regulation 2.0 (in force from 9 January 2025)**.

2. Purpose of the Policy

The objectives of this Policy are to:

- Ensure compliance with all applicable Curaçao laws and regulations relating to AML/CFT and Know Your Customer (“KYC”) requirements.
- Protect the Company, its employees, and its customers from being used as a channel for money laundering or terrorist financing activities.
- Establish clear and consistent procedures for customer due diligence, ongoing monitoring, reporting of unusual transactions, record keeping, and employee training.
- Define the responsibilities of the Money Laundering Compliance Officer (“MLCO”), management, and staff.
- Maintain a strong culture of compliance and integrity across the Company’s operations.

3. Scope and Applicability

This Policy applies to:

- All directors, officers, and employees of K.I.K Corporation B.V.

- All departments and functions, including Payments, Risk, Fraud, Customer Support, Compliance, and IT.
- All business relationships with customers, payment processors, and third-party service providers.

The Policy must be applied at all times and in all jurisdictions where the Company operates under its Curaçao license. The Company does not apply multiple sets of AML/CFT procedures per jurisdiction but ensures that all procedures are compliant with Curaçao legislation and international standards (FATF Recommendations).

4. Legal and Regulatory Framework

K.I.K Corporation B.V. is incorporated in Curaçao and bound by the following primary laws and regulations:

- **National Ordinance Identification when rendering Services (NOIS) (PB 2017, nr. 92)**
- **National Ordinance Reporting Unusual Transactions (NORUT) (PB 2017, nr. 99)**
- **National Ordinance on Offshore Games of Hazard (LOK) (PB 1993, no. 63)**
- **Indicators for detecting and reporting Unusual Transactions (PB 2015, nr. 73)**

The competent authorities overseeing AML/CFT compliance in Curaçao include:

- **Curaçao Gaming Control Board (GCB)** – supervisory body for AML/CFT in gaming.
- **Curaçao Gaming Authority (CGA)** – licensing and compliance authority.
- **Financial Intelligence Unit (FIU Curaçao)** – responsible for receiving, analyzing, and monitoring reports of unusual transactions.
-

International standards considered in this Policy:

- The **Financial Action Task Force (FATF) 40 Recommendations**.
- Relevant EU Directives transposed into Curaçao AML regulations.

5. Customer Due Diligence (CDD)

5.1 General Principles

K.I.K Corporation B.V. conducts Customer Due Diligence (CDD) on all players before establishing a business relationship or allowing financial transactions. The objective is to ensure that the Company knows its customers, understands their risk profile, and prevents misuse of its services for money laundering or terrorist financing.

CDD measures include:

- Identifying and verifying the identity of customers.
- Understanding the nature and purpose of the business relationship.
- Assessing the customer's risk level.

5.2 Identification and Verification

The Company requires all players to provide accurate identification details upon registration and prior to engaging in financial transactions.

Mandatory data collection includes:

- Full legal name.

- Date of birth (must be ≥18 years old).
- Nationality.
- Residential address.
- Valid government-issued photo identification (passport, national ID card, or driver's license).
- Proof of address (utility bill, bank statement, or other accepted documents – **only fixed-line telephone bills are accepted as proof of address** per GCB regulation).

Verification requirements:

- Documents must be valid and unexpired.
- Extra care must be taken when verifying **foreign documentation** unfamiliar to the Company.
- Sanctions and Politically Exposed Person (PEP) checks must be performed at onboarding (see Section 7).

5.3 CDD Thresholds

Under Curaçao law (amended May 2024):

- **CDD must be completed for financial transactions equal to or above NAf. 4,000 (≈ €2,000).**
- Financial transactions in online casinos include **deposits and withdrawals only** (bonuses and wagering are not financial transactions).

If the threshold is reached due to a deposit:

- The player may continue using existing funds, but cannot make further deposits or withdrawals until CDD is completed.

If the threshold is reached due to a withdrawal request:

- The account is frozen completely, preventing further play until CDD is completed.

5.4 Timing of CDD

CDD must be conducted:

- At the time of establishing a new business relationship.
- Before any financial transaction at or above the NAf. 4,000 threshold.
- On a risk-sensitive basis for existing customers who were previously exempt.
- Whenever there is doubt about the authenticity or adequacy of previously obtained customer identification data.

5.5 Simplified Due Diligence (SDD)

In low-risk situations, simplified CDD may be applied.

- Only basic identification details (name, date of birth, nationality, and unique player ID) must be verified.
- Further verification of additional personal details is at the Company's discretion, provided the Company has sufficient comfort that it knows the customer's true identity.

5.6 Enhanced Due Diligence (EDD)

Enhanced Due Diligence is mandatory when:

- A player is classified as high-risk (e.g., based on geography, unusual transactions, or payment methods).
- A player is identified as a Politically Exposed Person (PEP).
- Suspicious activity is detected during monitoring.

EDD measures may include:

- Collecting additional documentation on the customer's source of funds and wealth.
- Obtaining declarations signed by the player regarding the purpose of the relationship.
- Approval from senior management before establishing or continuing the relationship.
- More frequent and intensive ongoing monitoring.

5.7 Ongoing Monitoring of Customers

The Company continuously monitors all customer activity to ensure it is consistent with the player's profile and risk rating. Monitoring includes:

- Transaction reviews (daily, weekly, monthly reports).
- Tracking changes in customer behavior (e.g., sudden increase in deposits).
- Identifying suspicious transaction patterns such as multiple payment cards, third-party deposits, or unusual withdrawal activity.
- Ensuring customer identification documents remain valid (expiry tracking).

Monitoring reports include (non-exhaustive):

- €2,000 deposits in 24 hours – daily review.
- €10,000 deposits in 7 days – weekly review.
- €30,000 deposits in 30 days – monthly review.
- Multiple cards used within a short period.
- Low or no spending activity despite large deposits.

6. Monitoring of Transactions & Reporting to FIU Curaçao

6.1 Monitoring of Transactions

K.I.K Corporation B.V. maintains robust systems to monitor all financial transactions carried out by its players. Monitoring is both automated (system-based alerts) and manual (review by the Payments, Fraud, and Compliance Teams).

The monitoring system identifies unusual or suspicious patterns, including but not limited to:

- High deposit amounts (high volume or high value).
- Multiple payment methods used by the same customer.
- Use of third-party cards or accounts.
- Rapid changes in player behavior (deposit/withdrawal frequency, sudden spikes).
- Inconsistent gameplay compared to transaction levels.
- Deposits not turned over before withdrawal requests.
- Structuring (splitting transactions to avoid thresholds).
-

Monitoring is risk-based and ensures that unusual activity is escalated for further review by the MLCO.

6.2 Objective Reporting Indicators (FIU Curaçao)

The Company is legally required to report **objective indicators** of unusual transactions to the **Financial Intelligence Unit (FIU Curaçao)**.

Objective reporting applies when:

- **Any single transaction ≥ NAf. 5,000 (≈ €2,400 / USD 2,800) occurs in a gaming day.**
- This includes deposits, withdrawals, credit card payments, and e-wallet transactions.
- Prize payouts of ≥ NAf. 5,000 must also be reported.
-

Important:

- The NAf. 5,000 threshold applies **per gaming day**, not per individual transaction only.
- Bulk reporting is permitted, subject to FIU approval.

6.3 Subjective Reporting Indicators

In addition to objective indicators, the Company must report to FIU Curaçao when it has reason to suspect that a transaction may relate to money laundering or terrorist financing.

Examples include:

- Transactions inconsistent with a player's profile.
- Players unwilling to provide required identification or KYC documents.
- Use of multiple accounts or attempts to open duplicate accounts.
- Attempts to disguise the source of funds.
- Links to high-risk countries or sanctioned individuals.

All suspicious activity reports (SARs) are documented internally and escalated to the MLCO for review and filing with the FIU if deemed necessary.

6.4 Reporting Procedures

1. **Detection:** The Monitoring system flags unusual activity.
2. **Internal Report:** Employee raises an internal report via the Company's compliance reporting system.
3. **MLCO Review:** The MLCO reviews all supporting data, determines whether the case requires filing, and records the decision.
4. **FIU Submission:**
 - Objective indicators (≥ NAf. 5,000) → filed without discretion.
 - Subjective indicators → filed if suspicion of ML/TF exists.
5. **Record Retention:** All reports and FIU acknowledgements are retained for a minimum of 10 years.

6.5 Freezing and Blocking of Accounts

As required under the 2025 GCB AML Regulation 2.0:

- The AML program must specify **when reporting of unusual transactions will lead to blocking/freezing of player accounts.**
- Decisions must balance compliance with AML obligations and the **risk of "tipping off" the player.**
- Blocking may be applied in cases of confirmed suspicion, but the MLCO must always assess whether the action itself might compromise an FIU investigation.

6.6 Internal Escalation and Documentation

- Every suspicious case is logged in the Company's private compliance repository.

- Discussions and decisions by the Compliance Team and MLCO are documented.
- Audit trails must show the initial alert, the review process, and the final decision.

7. Politically Exposed Persons (PEPs) & Enhanced Due Diligence (EDD)

7.1 Politically Exposed Persons (PEPs)

All customers are screened against international sanctions and PEP databases **at onboarding**, before the business relationship is established. PEP screening is conducted simultaneously with sanctions screening, in line with Curaçao AML Regulation 2.0 (January 2025).

For ongoing relationships, screening is repeated regularly to capture any changes in customer status. If an existing customer is identified as a PEP, Enhanced Due Diligence (EDD) measures must be implemented **within 30 days**.

A **Politically Exposed Person (PEP)** is defined as an individual who is or has been entrusted with a prominent public function, including but not limited to:

- Heads of State, Heads of Government, Ministers, and Deputy/Assistant Ministers.
- Members of Parliament or equivalent legislative bodies.
- Members of governing bodies of political parties.
- Members of high-level judicial bodies or supreme courts.
- Ambassadors, senior officers in the armed forces, and central bank officials.
- Senior executives of state-owned enterprises.
- Members of the administrative, management, or supervisory bodies of international organizations.

Family members and close associates of PEPs are also treated as PEPs for the purposes of this Policy.

7.2 Enhanced Due Diligence (EDD)

Enhanced Due Diligence must be applied in the following cases:

- Customers classified as **high risk** based on geography, transaction behavior, or other risk indicators.
- Customers identified as **PEPs**.
- Customers exhibiting suspicious or unusual activity.

EDD measures include:

1. Obtaining additional information on the customer's source of wealth and funds, supported by reliable documentation (e.g., financial statements, payslips, contracts, inheritance documents).
2. Obtaining signed declarations from the customer regarding the purpose and intended nature of the business relationship.
3. Obtaining senior management approval before establishing or continuing a relationship with a PEP or high-risk customer.
4. Conducting more frequent and detailed ongoing monitoring of the relationship.
5. Where appropriate, obtaining third-party EDD reports from recognized providers.

7.3 Ongoing Monitoring of PEPs and High-Risk Customers

- PEPs and high-risk customers are subject to stricter ongoing monitoring than standard customers.

- Monitoring includes closer review of transaction patterns, payment methods, and gameplay activity.
- Any changes in the risk profile must be immediately escalated to the MLCO for reassessment.
- If the customer fails to provide required information or documentation within the prescribed timeframe, the account must be frozen and reported to the FIU where applicable.

8. Appointment of the AML Compliance Officer (MLCO)

8.1 Appointment

K.I.K Corporation B.V. has appointed a Money Laundering Compliance Officer (MLCO) who is responsible for overseeing the implementation and maintenance of this AML/CFT Policy. The MLCO is a senior member of management with sufficient authority, independence, and resources to carry out their role effectively.

A Deputy MLCO is also appointed to act in the absence of the MLCO.

8.2 Duties of the MLCO

The MLCO is responsible for:

- Implementing and monitoring compliance with Curaçao AML/CFT laws and regulations.
- Receiving internal reports of suspicious transactions and determining whether they must be reported to the FIU Curaçao.
- Filing objective and subjective reports to FIU Curaçao and maintaining all related documentation.
- Designing and updating internal AML/CFT procedures, including escalation protocols for freezing/blocking of accounts, taking into account the risk of tipping-off.
- Acting as the primary point of contact with regulatory bodies (CGA, GCB, FIU).
- Providing regular reports to the Company's senior management on the effectiveness of AML/CFT controls.
- Coordinating employee AML/CFT training and awareness programs.
- Ensuring annual reviews and audits of the AML/CFT program are carried out.

9. Training and Awareness

All employees of K.I.K Corporation B.V. receive training in AML/CFT obligations relevant to their roles.

Training includes:

- The provisions of Curaçao AML/CFT legislation (NOIS, NORUT, LOK).
- Internal reporting procedures and escalation channels.
- Employee liability and penalties for failure to report suspicious activity.
- Procedures for customer identification, verification, and ongoing monitoring.
- Recognition and handling of suspicious transactions.
- Case studies of recent money laundering and terrorist financing typologies.

New employees receive induction training before handling customer accounts. **Refresher training** is provided annually and whenever regulatory changes occur.

Records of all training sessions, including attendance and topics covered, are retained for a minimum of 10 years.

10. Record Keeping

The Company maintains comprehensive records in compliance with Curaçao legislation:

- Copies of all customer due diligence documents.
- Transaction records, including deposits, withdrawals, and internal alerts.
- Records of unusual transaction reports submitted to the FIU.
- Internal suspicious activity reports and MLCO decisions.
- Records of employee AML/CFT training.
- Audit reports and internal compliance reviews.

All AML/CFT records are retained for **at least 10 years** from the termination of the customer relationship or the completion of the transaction, whichever is later.

Records are stored securely in electronic and/or physical form and are accessible only to authorized personnel.

11. Independent Audit Function

In accordance with Curaçao AML Regulation 2.0 (2025), the Company maintains an **independent audit function** to test the adequacy and effectiveness of its AML/CFT program.

- The independent auditor must have at least **two years of experience** in AML/CFT compliance and hold a recognized AML certification (e.g., **CAMS, CAMS-Audit, or AMLFC**).
- The audit covers:
 - Customer due diligence procedures.
 - Monitoring and reporting systems.
 - MLCO effectiveness and decision-making.
 - Record-keeping and data retention.
 - Training adequacy.
- Findings are reported to senior management and corrective actions are implemented promptly.

12. Internal Reporting Procedures

12.1 Obligations of Employees

All employees must remain vigilant for suspicious activity and are required to report any knowledge or suspicion of money laundering or terrorist financing immediately to the MLCO.

Reports must include:

- Customer details.
- Transaction information.
- Nature of the suspicion.
- Supporting documentation.

Failure to report may result in disciplinary action and potential criminal liability under Curaçao law.

12.2 MLCO Procedures

Upon receiving a report, the MLCO will:

- Acknowledge receipt in writing.
- Review the report and supporting evidence.
- Determine whether it meets the threshold for filing with the FIU.
- File the report promptly if required, and retain FIU acknowledgements.
- Keep detailed records of decisions, whether a report was filed or not.

12.3 Prohibition of Tipping-Off

Employees are strictly prohibited from informing customers that a suspicious transaction report has been or will be filed. Disclosure of such information (“tipping-off”) is a criminal offense under Curaçao law and will lead to disciplinary and legal consequences.

12.4 Protection of Whistleblowers

Any employee making a report in good faith is protected from retaliation or adverse employment action. Reports are handled in strict confidentiality.

13. Risk Assessment & Business Risk Matrix

The Company conducts regular risk assessments of its operations, customer base, products, payment methods, and geographic exposure. A risk matrix is maintained to classify customers as **Low, Medium, High, or Not Accepted** based on:

- Customer profile and history.
- Jurisdiction and country risk.
- Transaction behavior.
- PEP or sanctions status.
- Source of wealth/funds.

High-risk customers are subject to EDD (see Section 7). Customers from prohibited jurisdictions or who refuse to provide mandatory KYC information are **not accepted**.

14. Employee Integrity & Screening

Before employment, the Company ensures integrity through:

- Verification of professional references and qualifications.
- Employment history checks.
- Criminal record checks, where legally permissible.
- Ongoing performance and compliance evaluations.

15. Policy Review

This Policy is reviewed annually by the MLCO, senior management, and the independent auditor. Updates are made promptly in response to:

- Regulatory changes in Curaçao.
- Findings from internal audits, external audits, or FIU feedback.
- Emerging risks or industry best practices.

The revised Policy is distributed to all employees, and training is updated accordingly.