

KLAVITORIX B.V.

V 1.0

KYC Policy

Document Information

Subject	KYC Policy
Purpose	Defines identity verification and risk management standards to ensure compliance with Curaçao NOIS and NORUT legislation
Involvements	All departments
Ownership	MLRO
Approval	Directors
Review	Annually or earlier as needed
Classification	Company Confidential

Change history

Date	Ver.	Author	Summary Changes	Director
14 May 2026	1.0	Anti-Financial Crime	New document created as part of AML/CFT Program review	

Contact information

In relation to any questions to the policy kindly contact IGA TRUST B.V. This policy is written to comply with the Curaçao CGA AML/CFT Guidelines for the Gaming Sector. Kindly note this policy is for internal purposes only and shall not be disseminated accordingly.

MLRO NAME

Director

Table of contents

Document Information	1
Table of contents	2
Purpose and Scope	4
Purpose of the Policy	4
Scope of Application	4
Service Provider Oversight	4
Governance and Responsibilities	5
Senior Management Responsibilities	5
Money Laundering Reporting Officer (MLRO)	5
AML/CFT/CFP Compliance Officer	5
Staff and Employee Duties	6
Timing of Customer Due Diligence (CDD)	7
Onboarding and Registration	7
Threshold-Based Triggers	7
Event-Based and Subjective Triggers	7
Ongoing Monitoring and Periodic Reviews	7
Documentation and Information Requirements	9
Initial Registration Information	9
Verification of Identity (Proof of Identity)	9
Verification of Address (Proof of Address)	9
Enhanced Due Diligence (EDD) Data	9
Management of Documentation Gaps and Relationship Termination	10
Handling of Missing Documentation and Information	10
The 30 Days Compliance Deadline	10
Termination of the Business Relationship	10
CDD and Risk Assessment Criteria	11
Customer Risk Assessment (CRA) Objective	11
Core Risk Factors	11
Risk Scoring and Categorization	11
Mandatory Escalation and Review Factors	12
Non-Acceptable Criteria	12
Ongoing Monitoring Framework	13
Objective of Ongoing Monitoring	13
Transactional and Behavioral Monitoring	13
Identification of Red Flags (Indicators)	13
Periodic Reviews and Data Refresh	14
Internal Escalation and Reporting	14

Politically Exposed Persons (PEP) Protocols	15
Definition of a PEP	15
Screening Frequency and Methodology	15
Review and Verification of Potential Matches	15
Risk Appetite and Action on True Matches	16
Sanctions Screening and Alert Management	17
Definition and Objective	17
Applicable Sanctions Lists	17
Screening Methodology and Frequency	17
Alert Review and Resolution	17
Procedures for True Sanctions Matches	18
Confidentiality and Reporting	18
Data Retention and Recordkeeping	19
General Principles	19
Retention Periods	19
Scope of Retained Information	19

Purpose and Scope

Purpose of the Policy

The primary objective of this Know Your Customer (KYC) Policy is to establish a robust framework for identifying and verifying the identity of [COMPANY NAME] customer base. This policy exists to:

- Ensure compliance with the National Ordinance on identification when rendering services (NOIS), the National Ordinance on the reporting of unusual transactions (NORUT), and other applicable Curaçao AML/CFT/CFP legislation.
- Prevent the Company from being used, intentionally or unintentionally, for money laundering, terrorist financing, proliferation financing, sanctions evasion, or other unlawful activities.
- Protect the integrity of the Company's online gaming services by ensuring that all participants are properly vetted at the start and during their relationship with the platform.

Scope of Application

This policy applies to all business activities, systems, and personnel under the control of [COMPANY NAME]. The scope specifically encompasses:

- Products and Brands: All online casino products and services offered through the domains operated under the Company's gaming license.
- Customer Types: All participants (players) who register or maintain an account on the platform, regardless of their assigned risk rating (Low, Medium, or High).
- Systems and Tools: The automated screening tools, transaction monitoring systems, and third-party identity verification (IDV) services utilized to execute KYC procedures.
- Teams and Departments: All employees

Service Provider Oversight

The Company utilizes technology partners and third-party compliance service providers for software integrity, identity verification, and PEP/sanctions screening. These providers are considered within the scope of this policy to ensure their processes align with the Company's risk appetite and regulatory obligations.

Governance and Responsibilities

Senior Management Responsibilities

Management is responsible for the day-to-day compliance with AML/CFT/CFP obligations within their respective areas. Key duties include:

- Resource Allocation: Providing the MLRO and Compliance Officer with appropriate resources to fulfil their functions effectively.
- Policy Approval: Ensuring the formal approval of the AML/CFT/CFP program, Business Risk Assessment (BRA), and Customer Acceptance Policy (CAP), Know Your Customer Policy(KYC).

Money Laundering Reporting Officer (MLRO)

The MLRO has complete autonomy in the suspicious activity evaluation process and unfettered access to all necessary information. Responsibilities include:

- Policy Ownership: Developing and maintaining policies in line with evolving statutory and regulatory obligations.
- Internal Review: Undertaking the internal review of all suspicions to determine if they require disclosure to the FIU.
- Decision Making: Making the final decision to refuse or terminate a business relationship

AML/CFT/CFP Compliance Officer

The Compliance Officer is tasked with the technical execution of the program. Responsibilities include:

- Procedural Operation: Operating procedures and controls for monitoring and testing compliance with AML/CFT/CFP legislation.
- Risk Management: Adopting and monitoring policies that manage the risks identified in the Business Risk Assessment.
- Reporting: Submitting at least an annual report to senior management describing industry developments and internal compliance activities.

Staff and Employee Duties

All employees, regardless of their role, are responsible for remaining vigilant to the possibility of money laundering. This includes:

- Reporting: Promptly reporting all knowledge or suspicions of money laundering to the MLRO.
- Compliance: Fully adhering to procedures regarding client identification, monitoring, and record-keeping

Timing of Customer Due Diligence (CDD)

Onboarding and Registration

Customer Due Diligence begins at the point of initial contact. The Company does not allow online gaming or the depositing of funds until the intended participant has registered personally, created an account, and confirmed their acceptance of the Terms and Conditions .

- **Mandatory Data Collection:** Registration will not take place if all required fields—including name, date of birth, nationality, and residential address—are not completed .
- **Account Activation:** No monies can be deposited and no bonuses allocated until the account has been activated via a link sent to the registered email address .
- **Initial Screening:** Automated tools identify Politically Exposed Persons (PEPs) and sanctioned individuals upon customer registration or deposit.

Threshold-Based Triggers

A mandatory requirement for gathering evidence to confirm identity is triggered when a participant reaches specific financial thresholds.

- **Qualifying Payments:** Verification is required when payments made to a participant exceed XCG 4,000 (or currency equivalent) in a single transaction or when they exceed XCG 4,000 cumulatively within a 30-day period.

Event-Based and Subjective Triggers

The Company re-applies or enhances due diligence whenever specific risks are identified, regardless of the financial threshold.

- **Suspicion of Underage Gaming:** If there is suspicion that a customer is underage and using adult details, further due diligence items must be requested .
- **Changes in Identity Information:** If changes are made to a customer's identity or personal information (such as a name change), full verification procedures are re-applied .
- **Risk Re-assessment:** The Customer Risk Assessment (CRA) is updated whenever material changes occur, such as a change in country of residence, use of new payment methods, or account dormancy followed by renewed activity .

Ongoing Monitoring and Periodic Reviews

Monitoring is a mandatory and continuous process for all accounts to ensure activity remains consistent with the customer's known profile and stated Source of Funds.

Formal periodic reviews of the Customer Risk Assessment are conducted based on the following schedule :

- High Risk: Every 12 months.
- Medium Risk: Every 24 months.
- Low Risk: Every 30 months.

Documentation and Information Requirements

Initial Registration Information

To establish a business relationship, every customer must provide the following personal details during the registration process:

- First and Last Name.
- Date of Birth (must be 18 or older).
- Email Address.
- Current Residential Address.
- Nationality.
- A chosen Username and Password.

Verification of Identity (Proof of Identity)

When verification is triggered, the Company requires a high-quality color scan of one of the following valid, unexpired, and signed government-issued documents:

- A Passport.
- A National Identity Card.
- An Armed Forces Identity Card.
- A Full Driving License.

Verification of Address (Proof of Address)

To verify a customer's place of residence, the Company accepts the following documents, provided they are no more than six months old and do not refer to a P.O. Box, including, but not limited to:

- A recent account statement from a recognized bank, building society, or credit card company.
- The most recent mortgage statement from a recognized lender.
- A recent rates, council tax, or utility bill (excluding mobile telephone bills, which are never acceptable).
- Official correspondence from an independent source, such as a government agency, or a lawyer's confirmation of property title.

Enhanced Due Diligence (EDD) Data

For customers deemed high-risk, additional information is requested to gain a deeper understanding of the relationship, including one or more pieces of evidence from, but not limited to, the list below:

- Documentation to establish Source of Wealth, such as a pay slip or a contract of employment;
- Documentation to establish Source of Funds, such as bank statement or e-wallet statement;
- Additional identification data such as former names, aliases, and previous addresses;

Management of Documentation Gaps and Relationship Termination

Handling of Missing Documentation and Information

The Company maintains a strict policy regarding the collection of required verification data. If a customer fails or refuses to provide requested customer due diligence (CDD), enhanced due diligence (EDD), source of funds, or source of wealth information without adequate justification, they are deemed unacceptable.

The 30 Days Compliance Deadline

Company staff are responsible for the ongoing tracking of accounts that have failed to meet verification requirements within the permitted window.

- If the required documentation is not received within 30 days of the initial request, Staff must confirm that all account restrictions (including the suspension of betting and payments) are active.
- As part of the 30-day escalation, staff will perform a high-level review of the account's transaction history. The purpose of this review is to identify and flag any specific behavioral indicators - such as a request for withdrawal followed by minimal or no gameplay - which Staff will then escalate to Compliance for further suspicion assessment.

Termination of the Business Relationship

In accordance with Article III.8 of the Curaçao AML Regulation, the Company must terminate an existing business relationship if it is unable to comply with applicable CDD requirements.

- Criteria for Termination: Grounds for termination include, but are not limited to:
 - Inability to verify the customer's identity or beneficial owner.
 - Failure to obtain sufficient information on the purpose and intended nature of the relationship.
 - Inability to complete EDD measures.
 - Reasonable grounds to suspect the relationship is connected to money laundering, terrorist financing, or proliferation financing where risks cannot be mitigated.
- Decision Authority: The decision to terminate a relationship is made by the MLRO
- Documentation: All termination decisions, including the supporting rationale and actions taken, are fully documented and retained.

CDD and Risk Assessment Criteria

Customer Risk Assessment (CRA) Objective

The Company performs a Customer Risk Assessment for every customer at the start of a business relationship and updates it continuously. The primary goal is to assess specific money laundering (ML), terrorist financing (TF), and proliferation financing (PF) risks associated with providing services to that specific individual.

Core Risk Factors

The customer's risk profile is formulated using data collected during registration, onboarding, verification, screening, and ongoing monitoring. The Company utilizes the following weighted factors to calculate a numerical Customer Risk Assessment score:

- **Country Risk:** Evaluation of the customer's residential address, nationality, and other jurisdictional connections.
- **Age Risk:** Identification of risks associated with the customer's age group.
- **Lifetime Risk:** Assessment of the total duration and history of the customer relationship.
- **Monthly Spending Risk:** Analysis of actual deposit and withdrawal volumes.
- **Payment Method Risk:** Evaluation of the specific payment service providers or methods used.

Risk Scoring and Categorization

Based on the calculated numerical score, customers are assigned to one of three risk categories :

Risk Category	Score Range	Requirement Level
Low	$0 \leq \text{score} < 20$	Standard CDD and ongoing monitoring
Medium	$20 \leq \text{score} < 50$	Standard CDD plus additional measures (e.g., enhanced monitoring)
High	$50 \leq \text{score} \leq 100$	Enhanced Due Diligence (EDD)

Mandatory Escalation and Review Factors

Certain indicators are not just weighted scores but require immediate manual review, escalation, or rejection. These include:

- Sanctions and PEP Exposure: Any match on global sanctions or PEP lists.
- Adverse Media: Negative news or public profile concerns.
- Transaction Behavior: Patterns suggesting structuring, pass-through activity, or third-party funding.
- Inconsistencies: Mismatches in identity details, location masking (VPNs/proxies), or linked-account indicators.
- Source of Funds/Wealth: Unresolved concerns regarding the origin of the customer's money.

Non-Acceptable Criteria

The Company will not establish or continue a relationship if the customer falls outside the defined risk appetite. This includes, but is not limited to:

- Confirmed sanctions matches.
- Confirmed PEPs, their family members, or close associates.
- Customers connected to prohibited or closed jurisdictions.
- Individuals suspected of acting on behalf of another person (mule accounts).
- Customers who fail or refuse to provide requested CDD or EDD information.

Ongoing Monitoring Framework

Objective of Ongoing Monitoring

Ongoing monitoring is a mandatory and continuous process designed to ensure that the Company's knowledge of a customer remains current and that their activity continues to align with their established risk profile. This process is essential for detecting unusual or suspicious patterns that may emerge after the initial onboarding phase.

Transactional and Behavioral Monitoring

The Company monitors customer activity on a continuous basis through both automated systems and manual reviews. This includes:

- Consistency Checks: Ensuring that the volume, frequency, and nature of deposits and withdrawals are consistent with the Company's knowledge of the customer, their business, and their risk profile (including Source of Funds).
- Automated Alerts: Utilizing system-based triggers to flag activity that deviates from normal patterns, such as sudden spikes in transaction volume or rapid turnover of funds.
- Payment Method Scrutiny: Monitoring for the use of multiple or third-party payment methods, and ensuring withdrawals are ideally sent back to the original source of deposit.

Identification of Red Flags (Indicators)

Staff are trained to recognize specific "Indicators" or "Red Flags" that suggest potential money laundering or suspicious behavior. Key typologies included in this monitoring are:

- Structuring (Smurfing): Multiple transactions just below the mandatory verification thresholds (e.g., NAF 4,000).
- Minimal Gaming Activity: Depositing large sums and requesting a withdrawal shortly after with little to no wagering ("Pass-through" activity).
- Inconsistent Behavior: Activity that does not match the customer's stated occupation or economic profile.
- Identity Masking: Frequent changes to personal details or the consistent use of VPNs/proxies to hide a player's true location.
- Collusion: Patterns suggesting that multiple accounts are linked or acting in a coordinated manner.

Periodic Reviews and Data Refresh

To ensure that Customer Due Diligence (CDD) information does not become outdated, the Company conducts formal periodic reviews of the Customer Risk Assessment (CRA) based on the following schedule:

- High Risk: Reviewed every 12 months.
- Medium Risk: Reviewed every 24 months.
- Low Risk: Reviewed every 30 months. During these reviews, the Compliance Team verifies that identity documents are still valid and that no new risk factors (such as negative media or PEP status) have emerged.

Internal Escalation and Reporting

If ongoing monitoring identifies activity that is deemed "unusual" or "suspicious," the following escalation process is triggered:

1. Detection: An employee identifies a red flag or an automated system generates a high-priority alert.
2. Internal Report: The employee or investigator completes an internal Suspicious Activity Report (SAR) detailing the grounds for suspicion.
3. MLRO Evaluation: The SAR is escalated to the MLRO, who has the final authority to determine if the matter requires an official filing with the Financial Intelligence Unit (FIU) Curaçao.
4. No Tipping Off: At no point during the monitoring or escalation process is the customer informed that they are under suspicion or that a report may be filed.

Politically Exposed Persons (PEP) Protocols

Definition of a PEP

A Politically Exposed Person (PEP) is defined as an individual who is, or has been, entrusted with a prominent public function. This includes:

- Heads of State, Heads of Government, Ministers, and Deputy or Assistant Ministers.
- Members of Parliament or similar legislative bodies.
- Members of the governing bodies of political parties.
- Members of supreme courts, constitutional courts, or high-level judicial bodies.
- Ambassadors, chargés d'affaires, and high-ranking officers in the armed forces.
- Members of the administrative, management, or supervisory bodies of State-owned enterprises.
- Directors, deputy directors, and members of the board of international organizations.

The definition extends to Family Members (spouses, partners, children, and parents) and Close Associates (individuals with joint beneficial ownership of legal entities or close business relationships).

Screening Frequency and Methodology

The Company performs PEP screening to ensure that no prohibited individuals are granted access to the platform.

- Onboarding Screening: Automated screening against global PEP databases is performed immediately upon customer registration or at the point of the first deposit.
- Ongoing Rescreening: All existing customers are subject to periodic automated rescreening on a daily basis to identify individuals who may have acquired PEP status after the business relationship was established.
- Adverse Media: Screening includes checks for negative news that may indicate a customer's political exposure or involvement in public-sector corruption.

Review and Verification of Potential Matches

All potential matches (alerts) generated by the automated screening system are subject to the following review process:

- Initial Analysis: The Compliance Team reviews the alert to determine if it is a "False Positive" (e.g., a common name) or a "Potential Match."
- Documentation: For potential matches, the Company may request additional data, such as a full middle name or a personal identification number, to confirm identity.
- MLRO Escalation: All "True Matches" are escalated to the MLRO for a final determination.

Risk Appetite and Action on True Matches

In accordance with the Company's Customer Acceptance Policy (CAP), confirmed PEPs, their family members, and close associates are not acceptable as customers.

- Rejection: If a PEP is identified during the onboarding phase, the application is rejected, and no business relationship is established.
- Offboarding: If an existing customer is identified as a PEP through ongoing monitoring, the relationship must be terminated.
- Documentation of Decision: The reason for rejection or termination is documented internally for audit purposes, but the customer is not informed of the specific PEP designation to avoid "tipping off."

Sanctions Screening and Alert Management

Definition and Objective

Sanctions are restrictions used by the international community to stop financial crime and terrorism. These measures are designed to change the behavior of targeted countries, regimes, or individuals when diplomatic efforts have failed. [COMPANY NAME] conducts screening to ensure it does not enter into financial transactions or provide services to sanctioned persons, as such individuals are outside the Company's risk appetite.

Applicable Sanctions Lists

The Company monitors several primary sanctions regimes to ensure global compliance:

- UN Sanctions: The UN Security Council list of individuals and organizations involved with terrorist activity (e.g., ISIL, Al-Qaeda) .
- EU Sanctions: Restrictive measures applied in pursuit of Common Foreign and Security Policy objectives.
- OFAC Sanctions: Economic and trade sanctions based on US foreign policy, which apply to all US dollar transactions .
- UK & Australia Sanctions: National autonomous lists administered by HM Treasury (OFSI) and the Australian Sanctions Office (ASO), respectively .

Screening Methodology and Frequency

- Initial Screening: Screening is performed with the help of automated tools to identify sanctioned individuals upon customer registration and/or deposit.
- Ongoing Monitoring: The Company recognizes that sanctions exposure may create increased risk and conducts re-screening on a daily basis through automated third-party tools .

Alert Review and Resolution

All screening alerts must be reviewed by the Compliance staff to distinguish between "False Positives" and "True Positives" .

- False Positive Outcome: If an analyst determines an alert is a false positive based on a comparison of identifiers (e.g., name, date of birth, nationality), the rationale is documented, and the customer may continue normal activity .
- True Positive Identification: If a true match is confirmed, the analyst must immediately inform and file an internal report to the MLRO.

Procedures for True Sanctions Matches

If an employee identifies a client as a sanctioned individual or entity, they must take the following immediate actions:

- Freeze Funds: Immediately freeze all funds and economic resources of the client available to the Company.
- Cease Activity: Do not enter into any further financial transactions or provide any services to the client.
- Account Suspension: Suspend the account until further instructions are provided by the MLRO.
- Enhanced Due Diligence: Apply EDD measures to fully document the match.
- Offboarding: Where a true positive is confirmed after onboarding, the account must be restricted and offboarded, subject to asset-freezing and reporting obligations.

Confidentiality and Reporting

- No Tipping Off: It is strictly prohibited to inform the client or any third party (except senior management or the MLRO) that a freezing measure is being applied or that an investigation is underway.
- External Reporting: If the MLRO determines there are reasonable grounds for the match, they are responsible for submitting the necessary information to the Financial Intelligence Unit (FIU) .

Data Retention and Recordkeeping

General Principles

The Company is committed to maintaining appropriate records of all participants and their associated transactions to ensure that an adequate audit trail is available for law enforcement and regulatory investigations. All internal compliance documents, including policies, risk assessments, and training records, are held within the secure back-office system with full access granted to the Money Laundering Reporting Officer (MLRO).

Retention Periods

In accordance with statutory requirements, the Company adheres to the following retention timelines:

- Customer Records: All identification records, standard/enhanced due diligence items, and financial transaction history are maintained for a period of 5 years after the date of account closure or the date of the last transaction.
- AML Registers: Records within the register of internal/external disclosures and the register of money laundering and financing of terrorism enquiries are kept for 5 years following the finalization of the relationship or as advised by the FIU.

Scope of Retained Information

The Company maintains secure daily backups of the following critical customer data:

- Registration and KYC: All registration details, identity verification evidence, and both standard and enhanced due diligence (EDD) items.
- Financial Data: A complete log of all deposits, bets made, withdrawals, prize payments, and bank reconciliations.
- Account Status: Records of suspended accounts (including reasons for suspension), closed accounts, and excluded players.
- Responsible Gaming: Details regarding self-exclusion periods (temporary and permanent) and self-imposed limits.
- Correspondence: All electronic communication records between Customer Service and the participant.
- Internal Investigations: Audit trails, internal reports, and notes on customer activity investigations.