

Know-Your-Customer (KYC) Policy

Genius Touch B.V.

(company number 160903)

version as of 01 July 2025

Approving Official:

Menno Jordaan, Director

Responsible Office:

Kaya W.F.G. (Jombi) Mensing 24 Unit A, Curacao

Effective Date: 01 July 2025

Next Review Date: 01 July 2026

1. General

GENIUS TOUCH B.V., a company formed under the laws of Curacao with registration number 160903 with registered office at Kaya W.F.G. (Jombi) Mensing 24 Unit A, Curacao (hereinafter to be referred to as “**Company**”, “**we**”, “**us**”, “**our**”) hereby adopts this Know-Your-Customer Policy (“**Policy**”) to demonstrate the main principles, methodology, and conditions that form a Company’s framework on prevention of money laundering (“**ML**”), terrorist financing (“**TF**”), and the proliferation of weapons of mass destruction (“**PF**”).

This Policy outlines the procedures and responsibilities the Company apply to successfully and timely detect any signs of the use of the Company’s services, products, or offerings for illicit activities such as money laundering, terrorist financing, fraud, and other financial crimes.

The Company is committed to forming, maintaining and upgrading transparent and compliant operational environment through adopting and integrating effective KYC measures into its core business activities. KYC measures are consistently applicable to players, business partners, all staff (both employees and contractors) and any other business relationships established by the Company, including but not limited to any service providers or third parties who process, review, or manage customer data and onboarding procedures.

This KYC Policy is applicable throughout the lifecycle of the customer relationship and extends to periodic reviews, monitoring, and suspicious activity reporting.

2. Legal Grounds

This policy is designed in accordance with the laws and regulatory guidelines of Curaçao, specifically:

- **National Ordinance on the Identification When Rendering Services (NOIS)** – Establishes the requirement to identify and verify the identity of customers before the provision of certain services.
- **National Ordinance on the Reporting of Unusual Transactions (NORUT)** – Sets out obligations to monitor and report unusual or suspicious transactions to the Financial Intelligence Unit (FIU) using the goAML system.
- **AML/CFT Supervision by the Curaçao Gaming Control Board (GCB)** – The GCB, acting under its supervisory authority, issues guidance and enforces compliance with AML/CFT obligations for entities operating under Curaçao gaming licenses.
- **GCB Requirements for Compliance Officer (Based on NOIS/NORUT)** – In accordance with the National Ordinance on Identification Services (NOIS) and National Ordinance on the Reporting of Unusual Transactions (NORUT), the GCB mandates the appointment of a designated Compliance Officer.
- **Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons** of mass destruction issued by Curaçao Gaming Control Board.

This policy also aligns with the best international practices, particularly those outlined by the Financial Action Task Force (FATF), to ensure a risk-based and globally consistent approach to KYC and AML/CFT compliance.

3. Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD)

The core measures of the KYC policy are CDD and EDD which are applied in accordance with the level of risk assigned to each customer under the Company’s risk-based framework. Depending on the results of KYC the player could be classified as low, medium or high risk level.

CDD comprises of the following actions:

3.1. Initial player due diligence. Prior to accessing any Company’s offerings, including demo accounts in games or bonus plays, the player shall complete the registration form by entering the following details:

- a. Username

b. Valid email address

As part of the registration, the player must explicitly confirm that they have read and agreed to the Company's Terms and Conditions and declare that they are of legal age to participate in gaming activities in their jurisdiction.

3.2. Full identification of player. Upon making first payment to the player's account, the Company requests the following player's data:

- Full name;
- Permanent residential address;
- Date of birth;
- Place of birth;
- Nationality;
- Government-issued ID number.

In low-risk situations, the Company could request three first personal details i.e. full name, date of birth and permanent residential address before the first deposit.

3.3. Verification of the player. Following the initial identification and preliminary customer risk assessment, the Company initiates a structured verification process to confirm the accuracy and legitimacy of the information provided by the player.

Upon the player's first payment or when otherwise deemed necessary based on risk level, the player will be required to submit reliable and independent documentation to verify their identity and residential address. This includes, but is not limited to:

- A valid government-issued identification document (e.g., passport, national ID card);
- Proof of residential address (e.g., utility bill, bank statement, or official letter from a public authority), not older than six (6) months.

In addition, the Company may request the player to complete one or more of the following verification steps:

- Email and/or phone number verification;
- A photograph of the player holding a handwritten note that includes:
 - The registered email address;
 - The current date;
 - A system-generated verification code.
- A photo of the player clearly displaying their identification document and the payment card used for transactions.

To enhance the accuracy of the player's risk assessment, the Company may also implement additional measures, including but not limited to:

- Biometric verification (e.g., facial recognition or any other liveness checks);
- Analysis of IP address and geolocation data;
- Screening of publicly available information such as social media profiles or government registries;
- Internal and external database cross-checks, including third-party screening services.

All verification procedures are conducted in accordance with this policy and the customer's assigned risk level under the Company's Risk-Based Approach.

3.4. Acceptable nature and purpose of the business relationship. The Company determines the nature and purpose of each player's interaction with the Company's offerings through carrying out risk-based assessment. The following indicators are assessed when forming the customer's risk profile:

- **Declared purpose of use**, which must be consistent with casual gaming and recreational betting, not investment or commercial activity;
- **Expected transactional behavior**, including frequency and volume of deposits, withdrawals, and gameplay activity;

- **Source of funds and source of wealth**, especially in higher-risk cases, which could be demonstrated through credible documentation such as:
 - Recent pay slips or income statements;
 - Bank statements showing salary or business-related income;
 - Tax declarations or notices of assessment;
 - Employment verification letters.

In addition, when **estimating the credibility of the declared source of wealth**, the Company may refer to the following:

- Public indicators of country risk (e.g. Transparency International, FATF listings, KnowYourCountry.com);
- Statistical data on minimum and average income in the customer's jurisdiction;
- Publicly available information on the customer's profession, position, or business ownership;
- Historical transaction behavior on the platform to identify discrepancies with stated income;
- Cross-referencing declared data with internal and external databases to detect anomalies or inconsistencies.

3.5. Ongoing Due Diligence and Monitoring. The Company monitors customers' activities on an ongoing basis to ensure that all transactions and behaviors remain consistent with the customer's established risk profile and do not expose the Company to money laundering, terrorist financing, or any other form of illicit activity. The monitoring consists of timely detection of suspicious behavior and suspicious transactions and if identified receiving CDD documentation necessary to explain such transaction and that the deviation from standard behavior or transactional pattern do not expose Company, its services or offerings to use in the money laundering or any other illicit activity. The basic patterns of suspicious activity include:

- a. using multiple cards from different payment agents,
- b. encountering specific error codes during payment,
- c. using cards issued by different emitters in different regions,
- d. using different payment instruments in a short period,
- e. being unwilling to verify account or payment information,
- f. inconsistencies in customer geolocation data,
- g. refusal to participate in phone or video calls and provide photo identification,
- h. matching device IDs with another account in the system etc.
- i. attempting multiple accounts with the website or with different websites operated by the Company.

The basic patterns of suspicious transactions include:

- a. If the transaction is made by using a payment card, the name of the holder shall be the same as the name of the website account owner. It means that any use of third-party payment card is prohibited;
- b. If the transaction is made by using an electronic wallet, this wallet's electronic mail may be the same that was used by a customer when registering an account on the Website;
- c. In case if a deposit is made from the payment instrument placement of funds to which is unavailable, the withdrawal shall be made to the customer's banking account or another payment instrument if it is possible to reliably ascertain that this payment instrument belongs to the customer in question;
- d. The Company does not withdraw funds that were deposited by the customer to the payment instrument of another customer.
- e. Uncooperative behavior during the Customer Due Diligence (CDD) process, such as being defensive;
- f. High spending amounts in comparison to the jurisdiction of the customer;

- g. Unnecessary queries about withdrawals, including withdrawals to third parties;
- h. In case the customer has multiple sources of income;
- i. In case the customer has irregular income stream;
- j. If players deposit a large amount but place no or small bets, followed by a request to withdraw all funds;
- k. Frequent deposits and withdrawals without any reasonable explanation;
- l. Significant changes in the customer's gaming patterns (depositing, wagering, or withdrawal behavior, etc.)

The list of patterns of suspicious behavior and suspicious transactions is inexhaustible and will be regularly supplemented in accordance with the detected suspicious activities and offerings updates.

The Company undertakes CDD in the following scenarios:

- When a player engages in a transaction equal to or above NAF 4,000 (or equivalent in another currency);
- When carrying out occasional transactions above NAF 4,000, including linked transactions which cumulatively exceed the threshold;
- When there is a suspicion of money laundering, terrorist financing, or proliferation financing;
- When the Company has doubts about the veracity or adequacy of previously obtained customer identification data.

Occasional transactions are typically associated with one-off interactions, especially in land-based settings, but are applicable to online operations when no formal account is opened.

EDD refers to more in-depth and rigorous checks applied to customers who present a higher risk of money laundering, terrorist financing, or other illicit activity. EDD goes beyond CDD and is designed to provide a deeper understanding of the customer's identity, financial background, and the purpose of the business relationship.

EDD measures are applied in the following circumstances, among others:

- **High-risk clients**, including Politically Exposed Persons (PEPs), Heads of International Organizations (HIOs), and individuals residing in or associated with high-risk jurisdictions as defined by FATF or EU regulations;
- **Customers engaging in large, inconsistent, or otherwise unusual transactions** that deviate from standard gaming or transactional behavior;
- **Clients using complex or opaque legal structures**, such as layered ownership, trusts, or shell companies, that may obscure the identity of the ultimate beneficial owner or the origin of funds.

For purposes of EDD, the Company shall collect information on

- Source of Funds ("**SO**F") – The specific origin of the funds used for a transaction or deposit (e.g., salary, company revenue, inheritance, investment income) and
- Source of Wealth ("**SO**W") – The origin of the customer's total wealth or net worth (e.g., business ownership, real estate holdings, long-term investments).

Documentation or evidence of SoF/SoW may include:

- Bank statements;
- Employment contracts or payslips;
- Tax returns;
- Sale agreements;
- Audited financial statements.

Where the source of funds or wealth cannot be reasonably verified, the relationship should be

rejected or terminated, and a Suspicious Activity Report (SAR) may be submitted to the Financial Intelligence Unit (FIU).

The Company may delegate third parties (such as financial institutions, law firms, or regulated entities) the aspects of the CDD process performance. The Company ensure that those third parties:

- The third party is subject to equivalent AML/CFT obligations;
- Written agreements are in place to ensure access to relevant documentation without delay;
- The company remains ultimately responsible for the customer's CDD and risk assessment.
- Third-party reliance must be documented and approved by the Compliance Officer.

4. Customer Acceptance Policy ("CAP")

The CAP set forth the conditions under which players are allowed to enter into or maintain a business relationship with the Company. The CAP exists and operates in conjunction with the customer risk assessment to ensure a risk-based approach to managing player onboarding and engagement.

The CAP supports the Company's compliance with its Anti-Money Laundering, Countering the Financing of Terrorism (AML/CFT), and Counter-Proliferation Financing obligations. It ensures that all customers are assessed consistently and in line with the level of ML/TF/PF risk they present.

The CAP has the following primary objectives:

- To ensure customers posing a higher-than-average ML/TF/PF risk are identified and subject to enhanced scrutiny;
- To categorize customers according to risk (low, medium, high);
- To determine and apply the appropriate level of CDD;
- To implement procedures for refusing or terminating relationships with unacceptable risk;
- To comply with regulatory requirements related to PEPs and Sanctions Screening;
- To align customer onboarding practices with the Company's risk appetite and regulatory environment.

The Company classifies customers into the following risk tiers, each of which requires a specific level of CDD:

Risk Level	Risk Indicators (Examples)	Applicable Due Diligence Measures	Company Response / Access Level
Low	– Customer resides in low-risk jurisdiction	Simplified CDD: • Standard identity info (name, date of birth, country, verified email) • Minimal frequency of updates to customer data • Reduced transaction monitoring within defined thresholds • Crypto wallet screening for source clarity	• Full platform access • Standard monitoring only • CDD refresh every 24 months unless triggered by risk change
	– Account activity aligns with expected profile (e.g., moderate deposits, regular gameplay)		
	– Complete and verified registration data (as per Section 6.1)		
	– Payment methods easily traceable (e.g., regulated financial institutions or verified crypto wallet)		
	– No PEP/HIO/sanctions exposure		

Risk Level	Risk Indicators (Examples)	Applicable Due Diligence Measures	Company Response / Access Level
Medium	– Customer resides in “monitored” jurisdiction (e.g., FATF grey list) – Deposit or bet volume increasing rapidly or inconsistently – Use of unregulated or semi-anonymous crypto wallets – Delayed response to verification requests – Cumulative deposits near or above NAF 4,000 – Doubts about prior submitted identity documents	Standard CDD: • Full identity documentation • Proof of address, source of funds • Sanctions, PEP, and HIO screening • Verification of submitted documents (manual or via third-party provider) • Transaction monitoring triggered when thresholds are reached	• Temporarily restricted deposit/withdrawal amounts • Full access granted upon successful CDD • Reclassification to High Risk if no response or unresolved discrepancies persist
		Enhanced CDD: • Verified ID + official proof of source of funds and wealth • Open-source and public domain searches for identity cross-check • Senior management approval before onboarding • Continuous enhanced monitoring • STR filing with FIU Curaçao • Screening through third-party tools (e.g., PEP/sanctions databases, crypto analytics)	• Access restricted or paused pending EDD completion • Deposit/withdrawals frozen until verification • Account flagged for monitoring by compliance team • FIU Curaçao report submitted if suspicion persists
High	– Customer resides in a “high-risk third country” (FATF or EU Delegated Regulation 2016/1675) – Politically Exposed Person (PEP), Head of International Organization (HIO), or close associate/family member – Unusual or concealed source of funds (e.g., privacy coins, mixers) – Cumulative transactions exceed NAF 4,000 without adequate verification		
Prohibited	– Customer listed on UN/EU/OFAC sanctions lists – Strong evidence of ML/TF activity – Fraudulent documentation – Repeated use of anonymizing tools (e.g., TOR, VPN) – Refusal to comply with CDD/EDD or unverifiable identity	Account Denial or Termination: • Onboarding denied or account suspended • Funds frozen if legally required • STR filed with FIU Curaçao • Record retention for 5 years	• Immediate termination of relationship • No access to platform services • Funds locked and reported as per AML laws

Risk Level	Risk Indicators (Examples)	Applicable Due Diligence Measures	Company Response / Access Level
		• Cooperation with law enforcement • Blacklisting and prevention of re-registration	

The Company reserves the right to refuse or terminate service under the following circumstances:

- The customer fails to provide satisfactory identification or CDD documentation;
- The customer is identified on a sanctions list or linked to a terrorist organization;
- The customer is non-cooperative or provides misleading information;
- The risk profile exceeds the Company's established risk appetite;
- The customer is associated with illegal activities or attempted ML/TF/PF.

PEPs and Sanctions Screening. In accordance with AML/CFT requirements, the CAP includes:

- Mandatory screening for all customers against PEP and sanctions databases at onboarding and regularly thereafter;
- Enhanced CDD and ongoing monitoring for identified PEPs and their close associates or family members;
- Immediate review and reporting obligations in the event a match is found with:
 - a. United Nations Sanctions Lists - <https://www.un.org/securitycouncil/content/un-sc-consolidated-list>;
 - b. OFAC, EU (<https://www.sanctionsmap.eu>), and other relevant bodies' lists;
 - c. Local regulatory or law enforcement watchlists.

PEP Screening sources include:

- Publicly available news sources
- The Transparency International Corruption Perceptions Index
- www.knowyourcountry.com
- PEP Caribbean List

Where a customer is identified as a PEP, EDD is applied, including:

- Senior management approval;
- Identification of the source of wealth/funds;
- Continuous enhanced monitoring.

Freezing of Funds and Reporting. If a player is identified as:

- A designated person under applicable sanctions;
- A PEP acting suspiciously;
- A high-risk individual linked to money laundering or terrorism;

Then the Company will:

1. Immediately freeze the player's account and block further transactions;
2. File an Unusual Transaction Report (UTR) with the Financial Intelligence Unit (FIU) Curaçao;
3. Avoid any action that could constitute tipping-off the player;
4. Document the reasoning and actions taken for compliance and audit purposes.

If the FIU determines the transaction is suspicious, it may refer the case for criminal investigation. The Company must not disclose to the player that a report has been made.

Risk Profile Updates. Each customer is assigned a risk classification (e.g., low, medium, high) during onboarding. This profile must be updated when:

- New information becomes available (e.g., change in ownership, business model, or residency);

- Suspicious behavior or transactions are detected;
- Trigger events occur (e.g., regulatory inquiries, adverse media).
- Changes to a customer's risk profile may result in enhanced monitoring, additional verification, or a decision to terminate the relationship.

Periodic reviews of customer profiles must be conducted at intervals proportionate to their risk classification:

- High-risk customers: annually;
- Medium-risk customers: up to every 2 years;
- Low-risk customers: every 2 to 5 years.
- The review process includes:
 - Re-validation of identification documents;
 - Updating contact and business information;
 - Re-assessment of the customer's source of funds;
 - Confirmation of ongoing alignment with expected activity.

Where discrepancies or red flags are identified, appropriate remedial actions must be taken, including escalation to the Compliance Officer and, if necessary, filing a Suspicious Activity Report (SAR).

5. Data Retention, Protection & Confidentiality

The Company is committed to maintaining the highest standards of data protection and confidentiality in handling customer information. All personal and financial data collected during the KYC and due diligence process must be securely stored, accessed only by authorized personnel, and protected from unauthorized disclosure, loss, or misuse.

This policy ensures compliance with applicable data protection, AML/CFT laws in Curaçao and relevant international standards

5.1. Storage of KYC Documents. All KYC-related documents and customer records must be:

- Stored in a secure, encrypted digital environment with restricted access;
- Backed up regularly to prevent loss or corruption;
- Retained for a minimum of five (5) years following the end of the business relationship or the completion of the last transaction, as required by the LID and LMOT;
- Made readily available to competent authorities (e.g., FIU Curaçao, Gaming Control Board) upon lawful request.

Documents include, but are not limited to:

- **Customer Identification Data:** including KYC documents, identification records, and verification information.
- **Customer Due Diligence (CDD) Files:** including risk assessments, source of funds/wealth checks, and beneficial ownership documentation.
- **Transaction Records:** including financial transaction history, payment logs, and internal audit trails.
- **Suspicious Transaction Reports (STRs):** both internally reported and those submitted to the FIU Curaçao.
- **Internal Investigation Files:** including notes, memos, or other documentation related to escalations or unusual activity.
- **Training and Compliance Logs:** records of AML/CFT training provided to staff and audit trails of compliance-related reviews.

The five-year period begins from the date of the last transaction or the termination of the customer relationship, whichever is later.

There an investigation is ongoing or records are requested by law enforcement or a regulator, the Company shall retain the relevant files until explicitly authorized to delete them..

Where hard copies exist, they must be stored in physically secure, access-controlled environments.

5.2. Data Privacy Alignment. Customer data must be collected and processed only for legitimate purposes related to customer due diligence, regulatory compliance, and risk management. The company commits to the following principles:

- Lawfulness, fairness, and transparency – Customers must be informed of the purpose for collecting personal data;
- Purpose limitation – Data is used strictly for AML/CFT, compliance, and related operational needs;
- Data minimization – Only information that is relevant and necessary for due diligence is collected;
- Accuracy – Customer data must be kept accurate and up to date;
- Integrity and confidentiality – Technical and organizational measures must be in place to protect data from unauthorized access or breaches;
- Right to access – Where applicable, customers may request access to their personal data, subject to legal limitations.

5.3. Secure Archiving Procedures. To protect the integrity, confidentiality, and availability of records the following rules apply:

- All documents shall be stored in secure, access-controlled environments, whether in digital or physical form.
- Digital records must be encrypted and backed up regularly on secure servers located in jurisdictions compliant with applicable data protection laws.
- Physical records (if maintained) must be stored in locked cabinets within restricted access premises.
- Access to archived records shall be limited to authorized personnel only, and any access or retrieval must be logged and auditable.
- The Company shall establish disaster recovery protocols to ensure data preservation in case of system failure or breach.
- At the end of the legally required retention period, documents may only be destroyed following a documented and secure disposal process, which includes:
 - a. **Digital files:** Secure deletion using data wiping tools;
 - b. **Physical files:** Shredding or certified destruction by an authorized provider.

6. Compliance Officer

6.1. Appointment & Responsibilities. The Company shall formally appoint a Compliance Officer (CO) at the senior management level. CO is independent from operational functions. The CO shall have timely and unrestricted access to all customer identification data, CDD files, transaction records, and other relevant documentation.

The CO will act independently and is entrusted with the following key responsibilities:

- Creating, implementing, and maintaining the Company's Policy;
- Conducting training sessions for the Company's staff related to the Policy;
- Developing and managing the risk management approach;
- Creating and revising policies, guidelines, and instructions for various departments of the Company within the Program;
- Submitting reports to the FIU as required by the "Reporting to FIU" provision;
- In certain cases, the Compliance Officer has the final approval within the Verification process;
- Communicating with the Company's counterparties regarding AML/CTF matters;
- Collecting, registering, processing and analyzing the data that it obtains in order to consider whether these data could be of any relevance for preventing and tracing money laundering or the financing of terrorism and the underlying criminal offenses;

- Providing data in accordance with the provisions laid down by or pursuant to the applicable regulation;
- Conducting investigations into developments in the field of money laundering or the financing of terrorism and into improving the methods to prevent or trace money laundering or financing terrorism;
- Giving recommendations, after consultation with the Supervisors or professional organizations in question, for the relevant business sectors regarding the introduction of fitting procedures for internal control and communication and other measures to be taken for preventing the use of relevant business sectors for money laundering or financing terrorism;
- Maintaining contacts with foreign police and non-police agencies, as stipulated by the authorities, that have a task that is comparable to that of the Reporting Office;
- Maintaining contacts with and participating in meetings of international and intergovernmental agencies in the field of combating both money laundering and the financing of terrorism.

6.2. Training, Independence & Fit-and-Proper Requirements. The Company, as per GCB guidelines, will establish fit-and-proper criteria for the Compliance Officer:

- At least 2 years of AML/CFT experience with a relevant degree or recognized AML certification (e.g., CAMS, AMLFC),
or
- At least 4 years of AML/CFT experience in a reporting role;
or
- Alternatively, 2 years of experience as an MLRO or equivalent role in another jurisdiction with knowledge of Curaçao's AML laws and familiarity with EU/OFAC sanctions list screening.

Any person considered for CO positions must align with mentioned requirements.

6.3. Conflict of Interest and Role Exclusivity. To ensure functional independence, the role of Compliance Officer must not be combined with the following positions:

- CEO, CFO, COO, UBO
- Casino Manager, Slot Manager
- Other operational, audit, or revenue-generating functions

The Compliance Officer role will remain fully independent and report directly to senior management or the board of directors.

6.4. Outsourcing and Jurisdictional Scope. The compliance function may be outsourced to a reputable third party, approved by GCB. The Company could provide outsourcing contract and qualifications of the responsible person/CO only upon GCBs request.

A Compliance Officer may act in the same role for multiple licensed entities, but no more than 10 operators (including roles in other jurisdictions), unless otherwise approved by the GCB.

Individuals may hold concurrent MLRO positions in other jurisdictions only if they have the time and capacity to fulfill all duties effectively.

6.5. Transitional Arrangements. If an appointed Compliance Officer does not fully meet established fit & proper criteria, the Company:

- Will immediately review personal history and integrity checks of candidate for CO;
- Will provide the assigned CO with 6 months timeline to eliminate any inconsistencies with responsibilities and independence requirements;
- Will provide the assigned CO with 12 months timeline to close any educational or experience gaps, subject to submission of a formal training plan for GCB monitoring.

Failure to meet those fit & proper criteria will result in CO resignation.

6.6. Suspicious Activity Reporting (SAR/STR). All employees will be trained to recognize indicators of suspicious behavior and escalate concerns to the Compliance Officer. Suspicious activity may include, but is not limited to:

- Unexplained changes in customer behavior or transaction patterns;
- Transactions inconsistent with the customer's known profile;
- Attempts to conceal identity or ownership structure;
- Use of third parties or proxies without clear justification;
- Use of high-risk or sanctioned jurisdictions.

If, after internal investigation, the Compliance Officer reasonably suspects that a transaction or activity involves criminal conduct, a Suspicious Activity Report (SAR) - also referred to as a Suspicious Transaction Report (STR) - must be submitted without alerting the customer.

SARs must be submitted promptly and in compliance with prescribed timelines and formats.

6.7. goAML System Usage All reporting of unusual or suspicious transactions must be conducted via the goAML portal - the official reporting platform of the FIU Curaçao.

Key goAML requirements include:

- Registration of the institution and Compliance Officer with the FIU;
- Secure login and controlled access to the system;
- Use of the appropriate reporting forms (e.g., objective vs. subjective indicators);
- Accurate and complete data entry;
- Timely responses to follow-up requests from FIU authorities.

6.8. Threshold-Based Reporting. Certain transactions must be reported to the FIU even if there is no suspicion of criminal activity.

These objective indicators are defined by law and include transactions that:

- Involve cash or equivalents above a specified monetary threshold (e.g., ANG 25,000 or its equivalent in foreign currency);
- Fall under transaction types explicitly listed by the FIU (e.g., international wire transfers over a set amount);
- Involve jurisdictions or sectors identified as high-risk by the GCB or FIU.

7. Employee Screening and Training Program

The Company commits to high ethical standards and compliance with financial laws through rigorous employee screening, including criminal background checks.

A comprehensive training program is provided to all employees who handle customer transactions or AML-related duties. Training is tailored by role:

- **New employees:** General AML/CTF awareness, internal policies, and reporting obligations.
- **Frontline staff (dealers, cashiers):** Specific training on recognizing and responding to money laundering risks in gambling operations.
- **Audit staff:** Updates on regulatory changes and AML enforcement.
- **AML Compliance staff:** Advanced training on emerging risks and regulatory expectations.
- **Supervisors and managers:** In-depth instruction on AML policies and oversight responsibilities.
- **Senior management and board:** Regular briefings on AML risks and reputational impacts. Refresher training is conducted regularly, and detailed records of all training activities, participants, content, and outcomes are maintained.

8. Periodic Review

The Compliance Officer shall ensure that the KYC/AML Policy is formally reviewed at least annually or more frequently under the following circumstances:

- Updates to applicable laws, ordinances, or guidance (e.g., NOIS, NORUT, GCB guidance);
- Changes in the Company's business model, product offerings, or risk exposure;
- Findings from internal audits, regulatory inspections, or compliance reviews;
- Material breaches or deficiencies identified in policy implementation;

- Emerging AML/CFT typologies, technologies, or industry risks.

The review process shall assess the continued adequacy, clarity, and effectiveness of the policy and associated procedures.

The results of each review, including proposed changes and rationale, must be documented and presented to senior management for approval.

9. Policy History

This is a new policy established to formalize the Company's AML and CTF framework in compliance with Curacao regulations.

Version 1.0

Effective Date 01 July 2025