

Anti-Money Laundering (AML) 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 duly incorporated and registered under the laws of Curacao, with registration number 160903, having its 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 Anti-Money Laundering and Know-Your-Customer Policy (the “**Policy**”) as a demonstration of its strong and ongoing commitment to combatting money laundering, terrorist financing, the proliferation of weapons of mass destruction and other illegal or fraudulent activity that may be conducted through use of the services of the Company. This Policy reflects the Company’s real intention to ensure full, effective and adaptable compliance with all relevant legal and regulatory obligations applicable to the gaming sector in Curacao.

This Policy is binding upon all individuals and entities engaged with the daily operations of Company, including but not limited to full-time and part-time employees, temporary staff, senior management and executives, contractors (including subcontractors and consultants), third-party suppliers, service providers, and any other persons or organizations that are acting under authority or on behalf of the Company.

This Policy applies to all aspects of the Company’s business activities, including but not limited to provision of the services related to offering the opportunity to participate in games of chance in the context of the operation of games of chance, casinos and lotteries and offshore games of chance. It extends to the delivery of such services across all online platforms and websites operated, owned, or otherwise controlled by the Company. When the Policy refers to a website it should be understood to encompass each and all websites operated by the Company. The Company is committed to ensuring that its anti-money laundering and know-your-customer standards are uniformly enforced across all operational channels.

The purpose of this Policy is to determine, declare and embed within the Company’s daily workflow a strict and adaptive framework of internal controls, risk-based procedures and CDD measures aimed at preventing, detecting, and responding to any attempt, act, or testing of the Company or its services for involvement in, or facilitation of, any illegal activity or the financing thereof.

LEGAL GROUNDS

This Policy has been created subject to the following laws, regulations, recommendations, guidelines, and rules:

- a. The provisions of Curacao`s legal framework, which include, but are not limited to:
 - The National Ordinance of the 2 October 2017, no. 17/2718 on identification when rendering services (“**NOIS**”).
 - Lands Decree of the 7th November 2017, no. 2017/3297 establishing the consolidated text of the National Ordinance on the Reporting of Unusual Transactions (“**NORUT**”).
 - The Sanctions National Ordinance (PB 2014, no. 55) and its bylaws
 - The Kingdom Sanction Act (N.G. 2016, no. 54)
 - Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction issued by Curaçao Gaming Control Board
- b. The Regulations and Guidelines of the Financial Action Task Force (FATF):
 - International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation (the FATF recommendations).
 - FATF Guidance on the RBA for Casinos.
- c. The legal framework of the European Union (to the extent applicable), which includes, but not limited to:
 - Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and supplementing Commission Delegated Regulations.

The Company undertakes all necessary actions for the compliance with this Policy, the NOIS, the NORUT, and the Sanctions National Ordinance, as well as other applicable regulation in the sphere of Anti-Money Laundering (AML)/ Counter-Terrorist Financing (CTF).

2. PRINCIPLES OF THE COMPANY

The Company employs the following principles to manage risks related to money laundering and terrorism financing:

- Conducting customer due diligence procedures depending on risks identified;
- Adopting a Risk Based Approach (RBA) to evaluate Money Laundering (ML) /Terrorism Financing (TF) risks;
- Implementing risk-based systems and procedures to monitor customers' ongoing activity;
- Reporting unusual transactions and other suspicious activity internally and externally to relevant law enforcement authorities;

- Maintaining records, including those related to internal investigations and external reporting, for the required minimum periods;

Providing training and screening to relevant employees and keeping them informed of the latest Anti-Money Laundering (AML)/ Counter-Terrorist Financing (CTF) legislation to ensure their awareness is always sufficient.

3. MONEY LAUNDERING AND TERRORISM FINANCING

For the purposes of this Policy, “**money laundering**” means as any intentional conduct that aims to conceal or disguise the nature, source, location, disposition, movement or ownership of the proceeds of a crime or property derived from an unlawful act, with the intention of using it in a legitimate or illegitimate way, or to assist any person who is involved in a crime to evade the legal consequences of their actions. Money laundering shall be regarded as such even where the activities which generated the property to be laundered were carried out in the territory of another country.

In turn, “**terrorist financing**” can be defined as providing, collecting or receiving of funds, whether directly or indirectly, with the intention that they be used, or in the knowledge that they will be used, in full or in part, to carry out terrorist acts. A terrorist act is defined as any act that involves the use of violence or threat of violence, or any other form of intimidation or coercion, for the purpose of advancing a political, religious or ideological cause, and that is likely to cause death, serious bodily injury or significant damage to property.

“**Financing of proliferation**” means the provision of funds for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials.

4. CORE MEASURES OF AML-CFT PROGRAM OF THE COMPANY

For ensuring the Company’s compliance with all applicable laws, statutory instruments of regulation, and requirements of the relevant supervisory body we apply the following measures:

- **Risk Assessment:** Company conducts periodic risk assessments to identify and mitigate potential AML risks in their operations.

- **Customer Due Diligence:** Company ensures performing of due diligence checks on all customers, including identity verification and screening against relevant AML databases. The type of due diligence checks mostly depend on the risks arising from the Company's relationships with a customer.
- **Suspicious Transaction/Activity Monitoring and Reporting:** Company ensures monitoring of transactions for suspicious activity and reporting of any suspicious transactions to the relevant authorities.
- **Record Keeping:** Company keeps records of all transactions and customer due diligence checks for at least 5 years.
- **AML Training:** Company ensures that all employees are trained on AML regulations and how to identify and report suspicious activity.
- **Regular monitoring of AML regulation changes and internal policies updates.** The Company uses utmost endeavors to make ongoing check of Task Force (FATF) and Caribbean Financial Action Task Force (CFATF)'s notifications, as well as monitor changes to the local AML regulation, on a regular basis and update their Customer Due Diligence policies and procedures accordingly to reflect these notifications and any changes.

5. RISK MANAGEMENT

In order to effectively manage our AML/KYC obligations, the Company adopts a risk-based approach. It hence identifies and analyses its risks and subsequently makes use of measures, policies, controls and procedures to mitigate any undesired risks, among which those related to the money laundering and funding of terrorism risks from materializing.

The Company applies a structured and documented methodology to classify risks as low, medium, or high. This methodology enables the Company to focus its AML/CFT measures on the areas/sections that pose the highest risk of ML/TF. The risk level of each customer is assessed when establishing a business relationship and continuously monitored throughout the relationship. The risk level of a customer may be adjusted at any time based on their activities.

Risk Management entails:

- i) recognition of existence of risk
- ii) undertaking of a risk assessment, and
- iii) implementing systems and strategies to manage and control the identified risks.

In order to assess the severity/level of risks, arising from relationship between you and the Company, we take into account the following factors:

a. Customer's Location:

The country (or place) of the customer's residence (jurisdiction) is evaluated on the following criteria:

- Whether the country of the customer's residence is specified in the list of "high-risk third countries with strategic deficiencies" of the Commission Delegated Regulation (EU) 2016/1675 and amending Delegated Regulations;
- Whether the country of customer's residence is specified in the list of "high-risk and other monitored jurisdictions" of the FATF;
- Countries on the CFATF Public Statement;
- Countries identified as Jurisdictions of Concern or Primary Concern in the U.S. Department of State's annual International Narcotics Control Strategy Report;
- Countries on the European Commission's list of third countries having strategic deficiencies in their AML/CFT regime;
- Countries sanctioned by the OFAC;
- Countries identified by credible sources as providing funding or support for terrorist activities or having terrorist organizations operating within them;
- Countries on the Corruption Perception Index compiled by Transparency International
- Additionally, the Company acts in good faith to implement its own list of high-risk countries (national risk assessment). The following factors are taken into consideration when creating the national risk assessment:
 - The legal system (the presence of independent legal institutions, rule of law etc.);
 - Political environment and political stability;
 - Cultural background;
 - Geopolitical factors;
 - The crime rate in a particular country

The customers are not allowed to receive the services at Company's web-site if they are from the countries that are historically prohibited by licensing conditions in Curacao, namely USA, Netherlands, France, Dutch West Indies and Curacao as well as any other countries which might be communicated by the Curacao Gaming Authority.

b. Product, service and Transaction Risk:

The Company ensures proper customer due diligence that anticipates, among other, second level of verification of the customer, i.e. sending of the valid identity documents, based on the risk assessment approach, among other, when the following conditions arise plus any other factors for the CDD procedure is in place:

- the amount of the deposit made through the website by a customer or the amount that will be released from the deposit reaches or exceeds NAF (ANG) 4,000.00 or its equivalent in another currency, notwithstanding whether such deposits have been carried out via a single operation or several operations which appear to be linked or otherwise.
- the amount paid for tokens (which includes chips and credits) sold to a client reaches or exceeds NAF (ANG) 4,000.00 or its equivalent in another currency

The Company may also initiate CDD if the customer requests to perform withdrawal of funds from the customer's account disregarding the amount of the withdrawal if the threshold is not established by the Company.

If, but is not limited to, a withdrawal transaction reaches or exceeds the threshold of EUR 10000 or its equivalent in another currency and any other conditions for enhanced Customer Due Diligence (CDD) described herein are met, the Company may initiate a conduct of enhanced CDD procedure.

The Company should also consider the following risk factors for their risk assessment and performance of the proper and reasonable required level of CDD:

- The use by customer of accounts held or cards issued in the name of third parties;
- The transfer of funds from one gaming account to another;
- Types of financial services used (credit/marker, currency exchange);
- Multiple casino accounts or wallets;
- Changes to financial institution accounts to fund casino account;
- Identity fraud. Details of financial institution accounts stolen and used on web sites. Also stolen identities used to successfully open financial institutions accounts, and such accounts used on web sites;
- Using cash to fund a pre-paid card;
- Games involving multiple operators (Poker on platforms shared by multiple operators);
- Use of Electronic wallets (e- wallets), e.g. not licensed in reputable countries, or accepting cash as deposits. Also, use of e-wallets which only accept money from financial institution accounts; the financial institution issued statements may only

record the payment to the e-wallet, not the transaction to the casino. This may be useful for dishonest customers who wish to disguise their gambling, etc.

c. Customer's behavior:

The Company exerts maximum diligence to perform ongoing monitoring of customer's activity on the Company's website to identify any suspicious behavior of each customer. Suspicious behavior may include, but is not limited to the following:

- High spending amounts in comparison to the jurisdiction of the customer;
- Use of multiple devices to log into the website in a short time frame or use of the same device or IP address by different customers;
- Uncooperative behavior during the Customer Due Diligence (CDD) process, such as being defensive;
- Unnecessary queries about withdrawals, including withdrawals to third parties;
- Attempts by a customer to register multiple accounts with the website or with different websites operated by the Company;
- Deposits that significantly exceed the usual gambling pattern of a customer;
- Depositing a large amount but placing no or small bets, followed by a request to withdraw all funds;
- Frequent deposits and withdrawals without any reasonable explanation;
- Significant changes in the customer's gaming patterns (depositing, wagering, or withdrawal behavior, etc.)
- Casual customers like locals/tourists, especially when spending pattern changes;
- Unknown customers (redeeming large amounts of chips);
- Junkets (junket operators monitor player activity and issues and collect credit);
- Customers who have multiple sources of income;
- Customers with irregular income streams.

d. Customer's status.

This relates to the type of customers being provided with the services. The assessment of the risk posed by a natural person is generally based on the person's status, economic activity and/or source of wealth. In identifying the level of risk inherent in a relationship, the Company will be assessing what would be the likelihood that a customer would be able to launder proceeds of crime through the Company's service.

Under the general rule a customer is prohibited to register or maintain an account with the Company's web-site if the customer is classified as a Politically Exposed Person ("PEP"), a Head of an International Organization ("HIO"), or a family member or close associate of a PEP or HIO ("PEP/HIO Related Person").

If during the CDD process the Company identifies that a customer is a politically exposed person (PEP) or Head of International Organization (HIO), or in any way associated to a PEP or HIO an enhanced CDD measures shall apply and upon the completion of the enhanced CDD measures the account will be closed at the Company's discretion.

The customer shall initially identify him/herself as not a PEP, HOI or PEP/HOI Related person to register on the Web-sites.

The Company ensures implementing of measures aimed at checking customers against the sanctions lists. Once identified, such customers are not allowed to use the services of the Company.

e. Technology risks

The Company shall take all possible efforts to monitor development of new technology and their potential use for the purpose of money laundering or the financing of terrorism.

Before introducing new products, services, business models, delivery channels, or implementing emerging technologies—including artificial intelligence—a thorough risk assessment must be conducted. The objective is to evaluate whether such innovations may introduce vulnerabilities that could be exploited for money laundering or terrorist financing purposes. Where any such risks are identified, the casino must adopt appropriate measures to manage and mitigate them effectively.

6. CUSTOMER DUE DILIGENCE

The customer due diligence developed by the Company enables the Company to:

- a. establish and verify the identity of a client;
- b. determine the purpose and intended nature of the business relationship and the services provided during the term of this relationship, monitor and investigate to ensure that they correspond to the Company's knowledge of its client and its risk profile, and, where necessary, investigate the source of the funds used in the business relationship or transaction;
- c. take risk-based and adequate measures to verify the client

Once the customer register on the Company's website, the latter performs initial CDD measures such as initial identification (collection of a series of personal details on the customer) and first level verification. Once identified, the customer is subject to ongoing monitoring of their activity.

If one of the triggers is revealed (both at the identification stage and later), the Company, depending on the nature and degree of risk's trigger, proceeds with either standard measures (like verification with submitting of the respective identity docs, including second level of verification) or enhanced measures (advanced identification and verification including a stringent check of the source of funds and the source of wealth). Until the applicable CDD process is successfully completed, all related transactions shall be suspended and remain unprocessed.

6.1. INITIAL CUSTOMER IDENTIFICATION

The Company does not allow to open and anonymous accounts of the customers.

Identification is the collection of information required to establish a customer's identity. Typically, a customer is initially identified by completing a registration form on a Company's website:

- a. Username
- b. Valid email address

The customer shall confirm that:

- he/she agrees with the Terms&Conditions at the web-site
- he/she is over 18 years old

Additional details could be requested in scenarios with higher risk level based on the risk assessment performed.

6.2. STANDARD CDD MEASURES FOLLOWING IDENTIFICATION

Standard CDD means additional identification of the customer followed by verification based on reliable documents.

In the cases specifically mentioned in this Policy and in other cases when, in view of the situation, at the sole discretion of the Company CDD measures are deemed necessary or when there are doubts about the veracity or adequacy of previously obtained customer's information the Company will ask the client to provide additional details and if considered necessary perform the verification process by submitting the identification documents.

The following data could be requested to this end:

- First Name and Last name
- Date of birth
- Residential address, including country, city, street and postal code
- Place of birth
- Nationality
- Identity number

This list could be limited to three first personal details from the above in low risk situations, i.e. full name, date of birth and permanent residential address that should be mandatory collected at least before the first deposit.

The following documents and data could be requested from a customer at the second level of verification:

Proof of identity: This may be a valid passport, travel document, driver license, identity card, or other government-issued identification document that includes the player's name, photo, date of birth, and other identifying information

It is important to note that the specific documentation requirements may vary depending on the individual circumstances of each player. Among other, the Company may request in addition:

- Proof of address: this may be a utility bill, bank statement, or other official document that shows the player's current residential address.
- Proof of payment: This may be a copy of the player's credit card, debit card, or other payment method used to make deposits or withdrawals.
- A photo of the customer bearing his/her identification document and payment card;
- If applicable - bank statement, the letter from the duty station or place of employment, tax bill;
- Photo of the customer holding a piece of paper with the requested information written by hand (the e-mail address of the customer, used when registering an account; the date of the photo request and the confirmation code);
- Other documents or information that may be required by the situation. In this case, a customer shall be additionally notified about the grounds of the request of this document, evidence or information.

The Company applies standard customer due diligence (CDD) based on the risk assessment approach, among other, when the following circumstances plus any other factors for the standard CDD procedure are in place:

- a. the amount of the deposit made through the website by a customer reaches or exceeds NAF (ANG) 4,000.00 or its equivalent in another currency, notwithstanding whether such deposits have been carried out via a single operation or several operations which appear to be linked or otherwise.
- b. the occasional transactions above the monetary equivalent of NAF (ANG) 4,000.00
- c. there is a suspicion of money laundering or terrorist financing
- d. there are doubts about veracity or adequacy of previously obtained customer identification data.
- e. A customer falls within another one or more risk categories specified in the "Risk Based Approach" section above.

The Company reserves the right to utilize specialized third-party providers for identification, verification, and screening purposes, including screening for Politically Exposed Persons (PEPs), Heads of International Organizations (HIOs), and sanctions. During the registration and verification process, we may transfer the information provided to the company to specific third parties to aid in and finalize the verification process.

6.3. ENHANCED CUSTOMER DUE DILIGENCE

The Company undertakes all necessary actions to conduct enhanced customer due diligence measures when such measures are required by law, or Company believes that such measures must be applied in order to establish the absence of illegal activity of the customer. Such measures may be applied when:

- a. The customer is a Politically Exposed Persons in the meaning of Article 3(9) of the Directive 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing or the customer is the member of the family of the Politically Exposed Person.

Under Article 3(9) of the abovementioned Directive, the Politically Exposed Person is a natural person who is or who has been entrusted with prominent public functions and includes the following:

- heads of State, heads of government, ministers and deputy or assistant ministers;
- members of parliament or of similar legislative bodies;
- members of the governing bodies of political parties;

- members of supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances;
 - members of courts of auditors or of the boards of central banks;
 - 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 or equivalent function of an international organisation.
- b. The customer is a Head of International Organization (HIO) is a person who currently holds or has held within the past five years the primary leadership role in an international organization or institution.

The organization or institution they head must either be: an international organization established by any state government, or (ii) an institution established by an international organization formed by any state government.

- c. The customer is a family member of a PEP or HIO includes: Spouse, common-law partner, ex-spouse, or former common-law partner, (ii) Biological or adoptive child(ren), (iii) Mother(s) or father(s), (iv) Mother(s) or father(s) of their spouse or common-law partner (mother-in-law or father-in-law), (v) Siblings.
- d. A close associate of a PEP or HIO encompasses individuals who:
- (i) Are business partners with, or beneficially own or control a business alongside a PEP or HIO;
 - (ii) Are in a romantic relationship with a PEP or HIO;
 - (iii) Engage in financial transactions with a PEP or HIO;
 - (iv) Serve on the same board as a PEP or HIO;
 - (v) Collaborate closely on charitable works with a PEP or HIO;
 - (vi) Are jointly listed on an insurance policy where one of the holders may be a PEP or HIO.

The Company uses services of the third parties to inspect whether a customer is a Politically Exposed Person or Head of International Organization.

- f. The country of customer's residence is specified in the list of "high-risk third countries with strategic deficiencies" of the Commission Delegated Regulation (EU) 2016/1675 and amending Delegated Regulations;
- g. The country of customer's residence is specified in the list of "high-risk and other monitored jurisdictions" of the FATF;

In addition to the standard Customer Due Diligence (CDD) measures, Enhanced Due Diligence (EDD) will be applied to the above customers. The EDD measures include:

- a. The customer will be required to provide documentation on the source of wealth and funds used to make deposits on the website.
- b. The customer's identity will be checked using open registers, social media, and other publicly accessible sources to verify the information provided by the customer.
- c. Senior management approval will be required before opening an account for a customer or continuing to operate an existing account.
- d. The Company will maintain ongoing, heightened control over the customer's relationship with the Company.

The Company will not provide services to a customer if it is known or reasonably assumed that the funds involved originate from corruption or the misuse of public assets, without prejudice to any legal obligations the Company may have under criminal law or other applicable regulations.

6.4. SIMPLIFIED CUSTOMER DUE DILIGENCE

In situations where the risks of money laundering or terrorist financing are deemed lower, the Company has the discretion to implement simplified CDD measures, which should be tailored to reflect the reduced risk level.

Examples of simplified CDD measures include:

- Decreasing the frequency of customer identification updates.
- Lowering the level of ongoing monitoring and scrutiny of transactions, based on a reasonable monetary threshold.

However, it's important to note that simplified CDD measures should not be employed if there is any suspicion of money laundering or terrorist financing, or in cases where specific higher-risk scenarios are identified.

6.5. ONGOING MONITORING

The Company monitors customers' activities for suspicious behavior on an ongoing basis, including using different payment methods or cards, getting error codes when making payments, and using payment cards issued by different issuers in different regions. Customers who refuse to verify their account or payment instrument, or those with mismatched geolocation information, may also be flagged. Transactions are also monitored to ensure compliance with

certain conditions, such as using a payment card with the same name as the account owner and not withdrawing funds to another customer's payment instrument.

Suspicious Activity Monitoring. All operations of customers are checked for the absence of suspicious activity on an ongoing basis. Suspicious activity includes, but is not limited to, the following:

- 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.

Transaction Monitoring. All the transactions of customers on withdrawal and deposits shall comply with the following conditions:

- 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.

7. REPORTING OF UNUSUAL TRANSACTIONS

The Company/ its Reporting officer submits reports to Curacao's Financial Intelligence Unit ("FIU") if the following indicator is in place:

- **Objective indicators.** They are not open to interpretation and rely on hard facts. When an objective indicator applies, the transaction must be deemed unusual and reported to the FIU. Objective indicators include:

- A transaction which is reported to the police or judicial authorities in connection with money laundering or the financing or terrorism.
- An intended transaction carried out by or for the benefit of a person, legal person, group or entity that is mentioned on a list compiled in pursuance of the Sanctions National Ordinance.
- A transaction amounting to NAF (ANG) 5,000.00 or more, regardless whether this transaction is carried out in cash, via a check or another payment instrument or electronically or in any other non-physical manner, covering:
 - A giro-based transaction amounting to NAF (ANG) 5,000.00 or more;
 - The taking into a deposit or the releasing out of the deposit of an amount of NAF(ANG) 5,000.00 or more, at the request of the client.
 - Sale of tokens to a client in the amount of NAF (ANG) 5,000.00 or more.
 - Payout of prizes in the amount of NAF (ANG) 5.000 or more.
 - All other cases
- ***Subjective indicator:***
 - A transaction giving cause to assume that it may be connected with money laundering or terrorist financing which may include, inter alia:
 - The customer refuses to pass the Verification, and the Company has ample grounds to suppose that such a customer presents a risk of money laundering or terrorist financing.
 - The customer`s transaction(s) or activity is suspicious (as mentioned above).
 - Additional indicators – any transaction with regard to which we suspect and have grounds to suspect that it:
 - involves funds derived from illegal activities;
 - is intended to evade taxes or other legal obligations;
 - is designed to avoid the reporting or other requirements under the gambling legislation;
 - has no apparent economic or lawful purpose;
 - involves the use of false or forged documents;
 - involves unusual patterns of transactions that have no apparent economic or lawful purpose;
 - involves the use of an account in a fictitious name;

- involves the use of an account that is held by someone other than the person conducting the transaction;
- is conducted in a manner that is inconsistent with the customer's known or declared business or financial profile.

The Company submits reports to FIU via the online reporting system **goAML**.

A reporting shall contain, insofar as possible, the following data:

- the identity of the client;
- the nature and the number of the identification paper of the client;
- the nature, the date and the place of the transaction;
- the amount, destination and origin of the funds, securities, precious metals or other values involved in the transaction;
- the circumstances on the basis of which the transaction is considered unusual.

Company understands and adheres to the restriction on the tipping off practices. In case the report is filled with FIU or any internal investigation is taking place, the customer shall not receive any of this information as such information may be used by the customer in order to “standardize” its behavior or activity or mitigate/destroy evidence needed for investigation

8. CUSTOMER ACCEPTANCE POLICY (CAP)

The CAP determines conditions under which players may enter into a business relationship with the Company, in alignment with the Risk Based Approach framework, to ensure that player engagement does not expose the Company to an unacceptably high risk of money laundering, terrorist financing, or related illicit activities.

In line with this approach, the Company reserves the right to take appropriate risk mitigation measures, including—but not limited to—restricting access to funds held on its platforms or temporarily or permanently suspending player accounts. Such actions may be taken where a player has been classified as high risk and has failed to provide the necessary documentation or take corrective measures required to eliminate or reduce the identified risk to an acceptable level. The Company applies the following rules:

Risk Level	Risk Indicators (Examples)	Applicable Due Diligence Measures	Company Response / Access Level
Low	– Customer resides in low-risk jurisdiction – Account activity aligns with expected profile (e.g.,	Simplified CDD (per Section 6.4):	• Full platform access • Standard monitoring only

Risk Level	Risk Indicators (Examples)	Applicable Due Diligence Measures	Company Response / Access Level
Medium	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	• 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	• CDD refresh every 24 months unless triggered by risk change
	– 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 (per Section 6.2): • 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 Enhanced CDD (per Section 6.3): • 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)	• Temporarily restricted deposit/withdrawal amounts • Full access granted upon successful CDD • Reclassification to High Risk if no response or unresolved discrepancies persist
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	• 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)	• 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

Risk Level	Risk Indicators (Examples)	Applicable Due Diligence Measures databases, crypto analytics)	Company Response / Access Level
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 • Cooperation with law enforcement • Blacklisting and prevention of re-registration	• Immediate termination of relationship • No access to platform services • Funds locked and reported as per AML laws

This Customer Acceptance Policy reflects the various customer due diligence scenarios and risk factors detailed throughout this Policy. Each individual case shall be assessed holistically, taking into account all relevant contextual, transactional, and jurisdictional factors to ensure a proportionate and compliant response as described hereto.

9. COMPLIANCE and REPORTING OFFICER

The Company appoints an AML Compliance Officer, who will serve as a Reporting officer for the unusual transactions as well. The Compliance officer has several responsibilities which include, but are not limited to, the following:

- 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;

The Reporting Office is granted authorization:

- To furnish the Supervisor with data and information pertaining to the reporting of reporting institutions, acquired in the execution of its assigned duties.
- Not to divulge identifiable information or disseminate statistics to individual service providers using data and information obtained in the execution of his assigned tasks.

10. EMPLOYEES SCREENING AND TRAINING

The Company will take all possible efforts to ensure its operations are conducted with high ethical standards and in full compliance with financial laws and regulations. The employees should be properly screened on reputational risks and criminal records before engagement.

The Company provides regular training and workshops for its employees/contractors as part of the Policy.

The training covers various topics such as :

- a. the Company's responsibilities under AML-CTF laws;
- b. how to identify suspicious transactions and activities;
- c. how to conduct verifications;
- d. who is considered a Politically Exposed Person etc.

Additionally, priority training is given to employees/contractors involved in standard CDD or enhanced CDD measures, and those who handle deposits or withdrawals, such as onboarding specialists, anti-fraud department, payment solution specialists, and support staff who deal with communication on withdrawal/deposit inquiries. The training may also cover other matters relevant to specific departments.

All new employees/contractors handling customer interactions or transactions—regardless of seniority—must receive basic training on money laundering and terrorist financing risks, the importance of reporting suspicious activity, and the Company's internal AML/CFT policies and procedures. They should also be trained on current methods and trends in the gambling sector, customer due diligence requirements, and indicators of suspicious behavior.

Audit Staff

Personnel responsible for monitoring and testing AML controls must stay informed on regulatory updates, enforcement actions, and evolving laundering methods affecting the Company.

AML Compliance Staff

Those managing the AML program require specialized training to keep pace with changes in risk and regulation. This may involve attending AML-focused events or conferences.

Supervisors and Managers

Staff in supervisory roles must receive advanced training covering all aspects of AML/CFT policies, procedures, and obligations.

Senior Management and Board

Risks and developments related to money laundering must be regularly communicated to senior management and the board of directors to ensure awareness and accountability at the highest levels.

11.RECORD KEEPING

The Company keeps records of the following data for a period of 5 (five) years from the date of the last transaction or the date when the customer has closed his/her account on any of the Websites:

- a. The information, obtained in the process of the verification and (if applicable) enhanced verification;
- b. The records of transactions (deposits, withdrawals) and their supporting evidence;
- c. The history of communications with customers of the websites;
- d. The data contained in the reports submitted to FIUs.

12.CONFIDENTIALITY

The Company will use utmost endeavors to keep the data collected during performance of this Policy and applicable AML/CFT regulation confidential. Anyone who supplies such data or information, and also the one who, submits a reporting on behalf of the Company, is obliged to maintain such confidentiality.

It is prohibited for anyone who performs or has performed any duties, to make use of such data further or otherwise, or to give publicity to such data further or otherwise, than for performing his duties.

13.RELIANCE ON THIRD PARTY

The Company may rely on third parties to perform certain elements of CDD, provided certain conditions are met. The third party must be subject to CDD and record-keeping obligations and have an independent business relationship with the customer. However, the Company retains full responsibility for compliance.

Key conditions include:

- Immediate access to CDD information from the third party;
- A formal agreement ensuring CDD documents are available on request, with periodic checks;
- Assurance that the third party is regulated and complies with CDD and record-keeping standards.

The Company must still conduct customer risk assessments, screen for PEPs, and ensure ongoing monitoring.

When determining in which countries the third party that meets the conditions can be based, casinos should have regard to information available on the level of country risk.

The Company is aware that it will remain responsible at all times for compliance with said regulations. For this reason there should be periodical assessments of how the service provider is fulfilling its obligations under the outsourcing arrangement both quantitatively and qualitatively. However, the decision whether to on-board a customer or to continue a business relationship on the basis of risk cannot be outsourced.

14. REVISION OF THIS POLICY

This Policy is subject to periodical revision. In addition, this Policy may be revised in the following cases:

- a. Changes in legislation;
- b. Changes in the corporate structure of the Company;
- c. Changes in the business profile of the Company;
- d. There are found sufficient deficiencies of this Policy;
- e. In other cases as applicable.

15. COMPLIANCE AND CONSEQUENCES OF NON-COMPLIANCE

The Company is committed to full compliance with all applicable Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) laws and regulations, including the National Ordinance on Identification of Clients when Rendering Services (NOIS), the National Ordinance on the Reporting of Unusual Transactions (NORUT), and relevant Sanctions Regulations.

All employees, contractors, and agents are expected to adhere strictly to the Company's AML policies and procedures. The Compliance Officer is responsible for ensuring the effective implementation, monitoring, and continuous improvement of the AML program.

Failure to comply with AML/CFT/CPF obligations may result in the following consequences:

- **Internal Disciplinary Measures:** Staff who fail to comply with AML requirements, whether through negligence or willful misconduct, may be subject to internal disciplinary action, including written warnings, suspension, reassignment, or termination of employment.
- **Regulatory Sanctions:** Non-compliance may lead to regulatory penalties imposed by the Gaming Control Board (GCB) or other authorities, including administrative fines, license suspension or revocation, and reputational harm to the Company.
- **Criminal Liability:** In cases of intentional or grossly negligent breaches, individual employees or Company officers may face criminal investigation, prosecution, and penalties under Curaçao law, including imprisonment and personal fines.

Mitigating Measures

To avoid such consequences, the Company will:

- Conduct regular training and awareness programs for all relevant staff;
- Ensure that the Compliance Officer and senior management monitor ongoing compliance;
- Require all personnel to immediately report suspected breaches or unusual activity;
- Review and audit the AML program regularly to identify and correct deficiencies;
- Cooperate fully with the GCB, FIU, and any competent authority during audits or investigations.

Employees are reminded that compliance with AML obligations is not optional and that ignorance of the rules is not a defense. It is every staff member's duty to uphold the integrity of the Company's operations and prevent its misuse for illicit purposes.

16.HISTORY

Date	Version
------	---------

01 July 2022	Initial Version 1.0
27 March 2024	Revised Version 2.0
01 July 2024	Amended Version 3.0
01 July 2025	Amended Version 4.0