

TH GAMBLING N.V.

**Anti-Money Laundering and Counter Financing of
Terrorism Policy and Procedure**

1. Contents

1. Contents	2
2. Abbreviations	4
3. Purpose	5
4. Policy	6
5. Procedures	6
6. Responsibilities	7
7. Risk Assessment	8
8. Customer Due Diligence	10
9. Sanctions Screening Policy	12
10. Politically Exposed Persons (PEP) Policy	13
11. Reporting of Unusual Transactions	15
12. Prohibited Countries	16
13. Employee Screening & Training	19
14. On-going Monitoring	20
15. Record Keeping	21
16. Continued Compliance & Accountability	21
17. Audit	21
18. Compliance Officer	21

Version Tracking, Release and Changes

Document Title	Anti-money Laundering and Counter Financing of Terrorism Policy and Procedure
Classification	Internal, Confidential
Version Control	V2.3
Last Updated	2025.07.15
Owner	Audrey Helstone
Date of Approval	2025.07.15

Signature

A handwritten signature in blue ink, appearing to be 'A. Helstone', is written inside a rectangular box.

2. Abbreviations

AML	Anti-Money Laundering
AML/CFT	Anti-Money Laundering and Counter Financing of Terrorism
BO	Beneficial Owner
BRA	Business Risk Assessment
CAP	Customer Acceptance Policy
CDD	Customer Due Diligence
CFT	Counter Financing of Terrorism
CRA	Customer Risk Assessment
EDD	Enhanced Due Diligence
EU	European Union
FIU	Financial Intelligence Unit
FT	Financing of Terrorism
FATF	Financial Action Task Force
KYC	Know Your Customer
CGCB	Curacao Gaming Control Board
ML	Money Laundering
ML/FT	Money Laundering and Financing of Terrorism
MLRO	Money Laundering Reporting Officer
PEP	Politically Exposed Person
PMLFT	Prevention of Money Laundering and Funding of Terrorism
RBA	Risk Based Approach
SAR	Suspicious Activity Report
UN	United Nations

3. Purpose

i. Introduction

This document has been compiled to create a core policy document to govern the various developed procedures and principles of the Company in one central location. This represents and ensures a prompt and up to date determined effort by the board of directors, senior management and the Company towards creating an appropriate framework and strategy to effectively prevent the misuse of the Company and its products and/or services for Money Laundering (ML) and Financing of Terrorism (FT).

ii. The Company

TH Gambling N.V. is a limited liability company registered under the Laws of Curacao on 22nd of May 2018. The company has its registered office at 6 Telamonstraat, Willemstad, Curaçao and its company registration number is 146982. It is authorized by the Curaçao Gaming Authority to offer games of chance under license number **OGL/2024/1468/1024**.

THBet B.V. is a limited liability company registered under the Laws of The Netherlands. The company has its registered office at Pastoor Petersstraat 3, Eindhoven, The Netherlands. Registration number: 67534716

iii. The Objective

The Company has set out this anti-money laundering (AML) and counter-terrorism financing (CTF) policy and procedure that is applicable to all staff to help prevent and detect potential ML/FT. The Company takes a zero-tolerance approach to ML/FT and other such financial crime.

The objective of this document is:

- To provide a high-level assessment of the operations and services provided by the Company and the risk that they may pose to ML/FT; and
- To set out the policies, procedures, systems and controls necessary for the Company to meet the obligations in Curacao.

The Company's approach is based upon:

- National Ordinance on identification when rendering Services (N.G 2017, no. 92);

- National Ordinance on the Reporting of Unusual Transactions (N.G 2017, no. 99);
- Sanctions National Ordinance (N.G 2014, no. 55)
- Kingdom Sanction Act (N.G 2016, no.54);
- Amendments on the first two bullet points made in P.B 2024, no. 41;
- Landsvordering van de 20ste December 2024 houdende regels betreffende kansspelen (P.B 2024, no 15).

4. Policy

It is the Company's policy that the statutory and regulatory obligations to prevent ML/FT are to be met in full and the Company is committed to meeting and where possible exceeding such obligations.

The Company will not onboard or continue established relationships with players whose conduct gives rise to suspicion of involvement with illegal activities. The Company will seek to suspend any player's relationship where the player's conduct gives reasonable cause to believe or suspect involvement with illegal activities. Upon identifying that any activity is being suspected to involve criminal/illegal activity, or there is knowledge to believe that the activity involves criminal/illegal activities, an investigation is to be completed and submitted to the Compliance Officer. If the Compliance Officer deems that a report needs to be filed with the FIU Curacao, the account needs to be suspended and no further transactions are to take place until further instructions are received from the FIU.

The Company's vigilance, policy and procedures are based upon the legislations and regulations referred to above and associated guidance issued by the Curacao Gaming Authority and the FIU.

In exercising the policy, the Company is committed to implement a compliance program consisting of the following pillars:

- A system of internal policies, procedures and controls;
- The appointment of a senior Compliance Officer/ MLRO;
- An employee screening program and ongoing employee training program, and
- An independent audit function to test the AML program;

5. Procedures

The purpose of these procedures is to assist the officers and employees of the Company in fulfilling their obligations under the Curacao statutory and regulatory obligations, thus ensuring effective implementation of the AML/CFT measures and mitigating risks. These will be maintained to ensure the following:

- The risk of the Company's products or services used as a vehicle for ML/FT is minimised;
- All players are properly identified and verified when necessary;
- New players who do not appear to be legitimate are declined, and where there is suspicion relating to criminal conduct on the part of a declined participant, such suspicion is reported to the Compliance Officer. Established participants' activities are regularly monitored to ensure that they fit the player's profile, especially in respect of large or abnormal transactions;
- Records are retained to provide an audit trail and adequate evidence to the law enforcement agencies in their investigations;
- All knowledge and/or suspicions are noted down in an internal investigation report (stored on confluence) and forwarded to the Compliance Officer. In turn, the Compliance Officer will review the report and gathered information and, if deemed necessary, submit a report to the FIU within two (2) days of having determined that the incident is reportable under the applicable indicator;
- Information on any internal investigation report is to be kept confidential and all internal investigation reports and external investigation reports together with any correspondence with the relevant authorities is to be retained by the company in a confidential manner;
- Full co-operation is provided to the law enforcement authorities to the extent required by statute/regulation. Furthermore, should a player of the Company come under investigation by law enforcement, the Company should be able to provide its part of any relevant audit trail, in respect of transactions and/or information about the player;
- That the Company's ongoing monitoring systems are implemented and regularly reviewed; and
- Appropriate knowledge and awareness are maintained regarding Curacao's statutory and regulatory obligations and in the gaming industry.

6. Responsibilities

The Company's board of directors and senior management are responsible for various matters such as:

- Setting the principles for the prevention of ML/FT, policies and the supporting procedures;
- Ensuring that the Company's policies and procedures are designed and operate effectively to manage the risk of the business from being used for financial crime and to fully meet the requirements of the AML/CFT regime;
- The appointment of a Compliance Officer who holds a sufficiently senior management role and expertise;
- Notifying the appointment of a Compliance Officer and a designated employee (if any) to the FIU and any other supervising authority as applicable;

- Ensuring that the Compliance Officer is promptly notified of unusual/suspicious transactions and other matters of significance;
- Ensuring that the Compliance Officer has complete autonomy in the suspicious activity report (SAR) evaluation process and unfettered access to information necessary to carry out the evaluation process; and
- Ensuring that the Compliance Officer is provided with or has access to the necessary resources (in terms of staff members and appropriate and up to date systems in place to detect suspicious activity and assist with conducting ongoing monitoring);
- Reviewing any recommendations made by the Compliance Officer concerning the Company's compliance with the relevant legislative framework and taking any necessary decisions thereon; and
- Approve the departments' documented operational procedures which procedures must be in line with the AML/CFT (among others) and as per requirements of the regulatory and supervisory authorities.

The Compliance Officer is responsible for ensuring compliance to the AML/CFT law with the requirements of the legal framework governing the Company. The Compliance Officer shall be afforded every assistance and cooperation by all members of staff in carrying out the duties to their appointment. The Compliance Officer is responsible for:

- Receiving reports from the employees of knowledge or suspicion of ML/FT, or that a person may have been, is or may be connected with ML/FT;
- Considering these reports to determine whether knowledge or suspicion of ML/FT subsists or whether a person may have been, is or may be connected with ML/FT;
- Reporting knowledge or suspicion of ML/FT or of a person's connection with ML/FT to the FIU;
- Responding promptly to any request for information made by the FIU; and
- Reporting any AML/CFT issues and matters to the Board of Directors.

Both the board of directors and the Compliance Officer will actively encourage other staff members to adhere to a strict compliance culture, where meeting processes and procedures set-out in this Policy are celebrated and rewarded.

7. Risk Assessment

The risk an action poses to the Company is determined by a Business Risk Assessment (BRA) and a Customer Risk Assessment (CRA). The higher the risk, the more measures the Company has to take to mitigate the risk. Where the risks are higher enhanced measures must be taken. Where the risks are lower, they may take simplified measures, provided that this is consistent with the country's assessment of its money laundering/financing of terrorism risks. Following risk segments have to be considering during the operation

i. Business Risk Assessment (BRA)

The BRA provides a detailed analysis of the ML/FT risks connected to the products offered by the Company, the payment methods it accepts, its customer base and the countries where the players are located or have an association with. Other qualitative and quantitative factors are also taken into account, such as the results from any national or supranational risk assessments. The controls put in place to mitigate the possibility that such risks materialize are assessed for their effectiveness.

In carrying out the BRA, the points outlined below are undertaken:

1. The identification and analysis of the inherent risk exposure of the Company across a wide range of categories such as its players, games, geographical areas, delivery channel methods and payment methods;
2. The determination of the level of risk that the Company considers acceptable;
3. The identification, analysis and testing of the AML/CFT controls in place to mitigate the inherent risk within the business undertaken by the Company;
4. The determination and quantification of the residual risk;
5. A remediation plan outlining the steps that are taken to reduce the level of risk (if necessary) in order to retain it within the risk appetite levels established by the Company's board of directors and senior management.

The MLRO is responsible for ensuring that the BRA is completed and reviewed at least annually, or whenever there are any regulatory or industry changes, and to reflect best practice and new trends. If following an annual review of the BRA, it has been determined that this is still current and valid, a note should be made that there is no need to update the assessment. Furthermore, once the BRA has been completed or revised in the years thereafter, it should be approved by the Board of Directors or the equivalent management body.

The BRA of the Company is to be made available to the relevant authorities upon request.

ii. Customer Risk Assessment (CRA)

To meet compliance standards it is important to have a policy that describes the types of players which are deemed to pose a low, medium or high risk of ML/FT, as well as the level of due diligence that is to be carried out (Minimum, Standard or Enhanced).

Whether a player poses a low, medium or high risk to the Company, depends on several factors.

Circumstances increasing customer risk:

- The player engages in high velocity/ aggressive gaming activity (can also be a risk from a responsible gaming perspective);
- A player is a resident of a higher risk geographical area;
- The player is an entrepreneur handling large amounts of cash;
- The player makes large value / volume transactions;
- The player is a PEP and/or subject to international financial sanctions and/or subject of negative news; and/or

Circumstances increasing product/service/transaction risk:

- The player engages in multiple transactions using high risk payment methods such as crypto, while depositing substantial funds;
- The player plays high-risk games and wagers little compared to the amount he deposits;
- The player plays games where it is easier to collude with others (e.g live casino blackjack).

Circumstances increasing geographical risk

- Countries identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective AML/CFT systems;
- Countries identified by credible sources as having significant levels of corruption or other criminal activity;
- Countries subject to sanctions, embargoes, or similar measures issued by the European Union (EU), United Nations (UN), United Kingdom (UK), or United States (US); and/or
- Countries providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country;

It is the combination of these factors that determine the type of Customer Due Diligence that is to be carried-out.

8. Customer Due Diligence

After having identified and assessed the risks that the players pose, the Company is to verify the players and apply CDD measures on a risk sensitive basis.

i. Minimum CDD-measures

Upon opening an account, the name of the user is requested and the Terms & Conditions need to be accepted. The name of the user is checked against:

- Being clearly fictitious;

- Sanction & PEP list, including the U.S. Treasury's Office of Foreign Assets Control's Specially Designated Nationals and Blocked Persons List (treasury.gov) and EU Sanctions List. (<https://www.sanctionsmap.eu/#/main>)

At the same time, the user accepts and acknowledges that he is the Ultimate Beneficiary Owner of the account.

ii. Standard CDD-measures.

When a User is categorized as Low or Medium risk, standard CDD is carried-out when the User:

- Transacts NAF 4.000 or more;
- Is suspected to be involved in money laundering or the financing of terrorism;
- Is suspected of having left fictitious or wrong details.

Standard CDD-measures are taken and the Identity of the User is verified and needs to send documents proving:

- Name & Surname;
- Residential address;
- Date and Place of Birth;
- Nationality;
- Identity Number.

Accepted documents are:

- Driver's License, Identification Card, Travel document or Passport;
- Bank Statement, Utility Bill, Correspondence from a central or local government, Rental Agreement.

A trained members of staff will assess the validity of the document and ensure the documents are not expired.

iii. Enhanced CDD-measures

When a User is categorized as High risk, enhanced CDD-measures are carried-out. At least one of the following actions are performed by a trained member of staff:

- Request more information from the customer (e.g occupation);
- Request more information on certain transactions / gameplay;
- Request Source of Wealth;
- Request Source of Funds.

Allowing a User that is categorized as High Risk to continue, can only occur after explicit Senior Management' approval.

iv. Failure to meet CDD

When a User fails to send the required documentation within 30 days upon requesting them, the business relationship is terminated. The User is notified of account closure, along with the reason (failure to meet CDD) and the account is locked until CDD is completed.

9. Sanctions Screening Policy

The Company is committed to fully complying with all applicable international sanctions regimes. As part of its Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) framework, the Company screens all customers and relevant third parties against the sanctions lists issued by the following official authorities:

- **United States (US)**

U.S. Department of the Treasury - Office of Foreign Assets Control (OFAC)

Specially Designated Nationals and Blocked Persons List (SDN)

<https://www.treasury.gov/ofac/downloads/sdnlist.pdf>

- **European Union (EU)**

EU Consolidated List of Financial Sanctions Targets

<https://www.sanctionsmap.eu/#/main>

- **United Kingdom (UK)**

HM Treasury - Office of Financial Sanctions Implementation (OFSI)

UK Sanctions List

<https://www.gov.uk/government/publications/the-uk-sanctions-list>

- **United Nations (UN)**

UN Consolidated Sanctions List

<https://www.un.org/securitycouncil/content/un-sc-consolidated-list>

i. Screening Requirements

The Company screens all customers against the above sanctions lists at the following stages:

- **At registration** - prior to account activation;
- **During ongoing monitoring**, at regular intervals and when lists are updated;
- **When changes occur** in a customer's personal data or activity that could affect risk classification;
- **When processing any transaction** exceeding the applicable reporting threshold or flagged as unusual.

ii. Positive Match Handling

If a positive or suspected match to a sanctioned individual, entity, or country is identified:

- The customer account is immediately suspended;
- All transactions are blocked;
- If a transaction took place; the Compliance Officer is notified;
- A report is filed with the FIU Curaçao, if required;
- No information is shared with the customer regarding the match or internal review, in accordance with anti-tipping-off obligations.

iii. Sanctioned and High-Risk Jurisdictions

Countries subject to full or partial sanctions by the US, EU, UK, or UN are considered **high-risk** or **prohibited jurisdictions**. The Company prohibits or restricts access from such jurisdictions in line with its internal risk appetite and regulatory obligations. This includes countries:

- Explicitly listed on any of the above sanctions lists;
- Associated with terrorist financing, organized crime, or corruption;
- Without effective AML/CFT regimes, based on credible assessments.

10. Politically Exposed Persons (PEP) Policy

The Company recognises the elevated risk of money laundering and corruption

associated with individuals who hold or have held prominent public functions, known as Politically Exposed Persons (PEPs), as well as their immediate family members and close associates. Enhanced scrutiny is applied to these individuals in accordance with international AML/CFT standards and Curaçao's legal framework.

i. Definition of a PEP

A **Politically Exposed Person (PEP)** is defined as a natural person who is or has been entrusted with a prominent public function, such as:

- Heads of state or government
- Senior politicians
- Senior government, judicial, or military officials
- Senior executives of state-owned enterprises
- Important political party officials

This definition also includes the following categories:

- **Immediate family members:** spouses, partners, children and their spouses/partners, and parents
- **Close associates:** individuals known to have joint beneficial ownership of a legal entity, or close business or personal ties

The definition of a PEP applies **regardless of residency or nationality**, and **remains applicable for a period of at least 12 months** after the individual ceases to hold the public function.

ii. Identification of PEPs

The Company identifies PEPs through:

- **PEP screening tools** integrated into the onboarding process
- **Manual checks** during Customer Due Diligence (CDD) for red flags or known affiliations
- **Regular updates from reliable databases.**

At a minimum, all new customers are screened for PEP status during account registration. This check is repeated periodically as part of the Company's ongoing monitoring obligations.

iii. Enhanced Due Diligence (EDD) Measures

Where a customer is identified as a PEP (or a close associate/family member of a PEP), the following **enhanced due diligence (EDD)** measures are applied:

- Obtain approval from **Senior Management** before establishing or continuing the business relationship;
- Take reasonable measures to establish the customer's **source of wealth and source of funds**;
- Conduct enhanced, **ongoing monitoring** of the customer relationship, including review of transaction patterns and red flags;
- Maintain clear internal documentation of the PEP classification, decisions taken, and actions performed.

EDD measures must also be applied to PEPs identified **after** the customer relationship is established.

iv. Risk Management

Customers identified as PEPs are automatically classified as **High Risk** within the Company's Customer Risk Assessment (CRA) framework. As such, they are subject to a higher level of scrutiny and review.

If at any point the relationship is deemed to present an unacceptable level of risk, it shall be declined or terminated in accordance with the Company's AML procedures.

v. Record Keeping and Confidentiality

Records of all PEP screening, decisions, and enhanced due diligence measures are maintained in accordance with Section 12 of this policy and retained for a minimum of five (5) years after the relationship has ended. All information shall be treated as confidential and only disclosed to relevant authorities upon request or legal obligation.

11. Reporting of Unusual Transactions

It is mandatory to report Transactions that are Unusual. Unusual transactions are:

- A transaction (deposit or withdrawal) over Naf 5000 (~€2.500) -> Objective Indicator;

- Transactions by Users which are being investigated by to the police in connection with Money Laundering/ Terrorism Financing -> Objective Indicator
- Transaction by a person on the sanctions list -> Objective Indicator.
- Transaction flagged by the Compliance Officer in connections with Money Laundering -> Subjective Indicator.

Variables a Compliance Officer may consider when labelling a transaction as unusual:

- User has more than one account in his name;
- Withdrawals without genuine gameplay (just betting the deposited amount 1x to meet Terms);
- Even Money Betting;
- Requesting to exchange Fiat to Crypto to a member of staff;
- Other risk-increasing factors as outlined in the CRA-section.

When a Transaction is Unusual due to an Objective Indicator, it needs to be submitted within **48 hours** of the transaction taking place.

When a Transaction is Unusual due to a Subjective Indicator, the Compliance Officer has 10 working days to determine and research whether the transaction needs reporting or not.

It is the responsibility of the Compliance Officer to report these Unusual Transactions to the FIU Curacao.

12. Prohibited Countries

The Company does not onboard or maintain relationships with individuals or entities residing in, or otherwise associated with, jurisdictions that present an unacceptable level of risk in relation to Money Laundering, Terrorism Financing, or are subject to comprehensive sanctions. This includes countries and territories identified through:

- Sanctions issued by the **United Nations (UN)**, **European Union (EU)**, **United States (OFAC)**, and **United Kingdom (OFSI)**;
- Regulatory restrictions applicable to the Company's payment providers and financial institutions (e.g., Bilderlings);
- FATF-designated **High-Risk Jurisdictions subject to a Call for Action or Jurisdictions under Increased Monitoring**;
- The Company's own **Business Risk Assessment (BRA)** and internal risk appetite.

Players attempting to register or operate from the following countries will be automatically declined or blocked, and existing accounts will be suspended and reviewed:

i. Prohibited Jurisdictions

Country / Region	Reason
Afghanistan	Sanctions / Terror Financing Risk
American Samoa	FATF / Sanctions
Barbados	FATF / Tax Transparency Risk
Botswana	FATF
Burundi	Sanctions / AML Deficiency
Cambodia	FATF
Central African Republic	Conflict / Sanctions
Cuba	US Sanctions / Financial Restrictions
Democratic Republic of Congo	Sanctions / Conflict Financing Risk
Crimea Region	International Sanctions
Ethiopia*	Card Scheme Restriction (e.g., Mastercard)
Fiji	FATF / Risk Jurisdiction
Guam	FATF
Iran	Comprehensive International Sanctions
Iraq	High ML/TF Risk
Lebanon	High ML/TF Risk
Libya	UN / EU Sanctions

Country / Region	Reason
Mali	Sanctions / Conflict
Myanmar	Sanctions / Military Regime
Nicaragua	Political / AML Sanctions Risk
North Korea	Global Sanctions
Pakistan	FATF Watch List
Palau	FATF
Palestine	Conflict Risk
Russia	Sanctions / Ownership restrictions ($\geq 25\%$)
Belarus	Sanctions / Ownership restrictions ($\geq 25\%$)
Samoa	FATF
Somalia	Terror Financing / Sanctions
South Sudan	Conflict / UN Sanctions
Sudan	Conflict / Terror Financing
Syria	Comprehensive Sanctions
Trinidad and Tobago	FATF
Uganda	FATF
Venezuela	US / EU Sanctions
Yemen	Conflict / Terror Financing
Zimbabwe	Sanctions / AML Risk

** Applies to restricted card services (e.g., Mastercard)*

ii. Ongoing Review and Dynamic Risk Management

This list is **not exhaustive** and is subject to continuous review and revision. The Company maintains a **dynamic and risk-based approach**, meaning the list of prohibited jurisdictions evolves in line with:

- Changes to international sanctions regimes;
- FATF assessments and grey/blacklists;
- Developments in political risk, conflict, or regulatory guidance;
- Updated risk appetite or payment provider restrictions.

13. Employee Screening & Training

The Company represents an amalgamation of appropriately qualified people and past-paced technological innovation. Employees are one of the most valuable assets and a critical component of the Company's operating model. In an intense, gain-driven betting environment, staff reliability and probity are of paramount importance to an extent unseen in other businesses.

The Management of the Company recognizes this and, therefore to ensure the highest standards of professionalism and integrity, all prospective employees must provide a valid clean bill of conduct prior to employment. This verifies their eligibility and suitability to perform in their designated roles.

Employees are expected to:

- conduct their activities in accordance with direct instructions of the immediate supervisors
- exercise sound judgment in situations requiring initiative and unsupervised decision-making
- behave ethically towards the Company, colleagues, clients and third parties
- be fair, honest, dependable and accountable in business dealings
- avoid business and personal actions that might cast appearance of impropriety or ethical ambiguity
- comply with the respective HR policies and regulatory requirements

- declare any actual or perceived conflicts of interest as soon as such conflicts become known
- maintain confidentiality and prevent the disclosure of the confidential information
- refrain from accepting inducements, incentives, gifts or other benefits from the colleagues and third parties that may lead to, or may be seen as leading to, an unfair advantage to third parties or to unfair treatment of the business
- communicate internally and with the third parties using clear and concise meanings, in a timely manner and via the established communication channels
- decline invitations from the mass media and the Internet-based platforms (forums, info-aggregators, news originators and others) to discuss the Company's business.

Additionally, we are committed to continuous professional development by implementing regular training programs tailored to the needs of their roles. These sessions will, amongst others, focus on compliance with the processes and procedures outlined in this document, but also in the varied subject areas of direct interest to the business.

The Company will maintain a log with all training records.

14. On-going Monitoring

On-going monitoring is conducted by the Company in order to ensure that the information collected about the player at registration stage, is still current and valid and to determine whether there is any suspicious activity that requires further investigation.

In conducting ongoing due diligence on the business relationship, the Company holds accurate and up to date identification data of its customers. Since identity may change due to circumstances, the information must be detected and re-evidenced. The Company requests evidence of identity periodically to detect any changes, refresh the data on key events (i.e., change of payment instrument) or tracks expiry dates on evidence of identity and refreshing it as it expires. The

Company determines on a risk-sensitive basis whether changes are substantial as to require re-assessment of customer risk of the business relationship.

15. Record Keeping

Documents are stored securely on our Curacao Servers and backed-up on secure back-up servers. Documents are in theory never removed, but should the need arise, it will never affect documents that have been submitted less than 5 years ago from the deletion initiative.

16. Continued Compliance & Accountability

This Policy is reviewed annually and formally approved by the Board of Directors.

17. Independent Audit

The AML compliance program will be evaluated at least annually by the internal audit department or an outside independent party. The audit is to assess and consequently ensure that the Company's policies and procedures are in line with the regulations and thus adhered to.

18. Compliance Officer

The Company will appoint a Compliance Officer, goes by the name of Audrey Helstone and his responsibilities are a.o., the following:

- Ensure compliance with Curacao Gaming Authority regulations and relevant AML/CFT laws.
- Maintain awareness of the legal landscape in Curaçao, including licensing conditions and regulatory updates.
- Implement and oversee compliance policies and procedures in line with industry standards.
- Conduct risk assessments on high-risk customer profiles and ensure appropriate monitoring and reporting.
- Map product-related risk exposures (payment methods, product verticals, casino categories, etc.).
- Map customer-related risk exposures (deposit/withdrawal ratios, wagering-to-deposit factors, geographical risks, etc.).
- Analyze transactions and verify whether any are subject to reporting according to the indicators referred to in the LvMOT;
- Review all internally reported unusual transactions for their completeness and accuracy;

- Report unusual transactions to the Financial Intelligence Unit (FIU) in compliance with AML/CFT guidelines.
- Keep records of all internally and externally reported unusual transactions;
- Request and verify RNG (Random Number Generator) certificates from third-party game providers.
- Review and ensure that Terms & Conditions align with internal policies and regulatory requirements.
- Collaborate with internal teams to implement compliance initiatives and provide training when necessary.
- Maintain records of compliance activities and provide reports to senior management and regulatory bodies as required.