

Trigonon Group B.V.

Anti Money Laundering (AML) Policy

Table of Contents

1. Policy Statement.....	3
2. Policy Purpose	3
3. Definitions.....	4
4. Policy Implementation.....	6
4.1. Senior Management Responsibilities	6
4.2. Compliance Officer	6
4.3. Employee Conduct And Support	7
4.3.1. Staff Integrity And Screening	7
4.3.2. Training And Awareness.....	7
5. Risk based Approach (RBA).....	7
5.1. Business Risk Assessment	8
5.2. Customer Risk Assessment	9
6. Customer Acceptance Policy.....	10
6.1. Sanctions.....	10
7. Customer Due Diligence.....	11
7.1. Customer Identification	11
7.1.1. Registration Procedure	12
7.2. Verification	12
7.2.1. Email Verification Process.....	12
7.2.2. Mobile Verification Process	13
7.2.3. Customer Due Diligence (CDD)	13
7.3. Enhanced Customer Due Diligence (EDD).....	15
7.3.1. Politically Exposed Persons (PEPs)	15
7.4. Monitoring	16
7.4.1. Ongoing Customer Profile Monitoring.....	16
7.4.2. Ongoing Transaction Monitoring	16
8. Reporting of Unusual Transactions	17

8.1.	Reporting Obligations	17
8.2.	Recognition of Unusual Transactions	17
8.3.	Prohibition of Disclosure.....	18
8.4.	Record Keeping.....	18
9.	Anti-Money Laundering Compliance Program.....	19
9.1.	Appointment of a Compliance Officer	19
9.1.1.	Duties of the Compliance Officer	19
9.2.	Employee Screening and Training Programs	19
9.2.1.	Employee Due Diligence	19
9.2.2.	Training	20
9.3.	Independent Audit Function	20
9.4.	Examination by the Curaçao Gaming Authority	21
10.	Compliance and Consequences of Non-Compliance	21

Document Information:

Approval	Board of Directors
Responsible Office	Compliance Officer
Review	Annually
Audience	All Employees, Contractors, and Third Parties
Effective Date	April 10, 2025
Next Review Date	May 30, 2026

Policy History

Date	Version	Summary Changes	Approved by Management
	1.0	Policy implementation	

For any questions regarding this policy, please contact the designated Compliance Officer.

1. Policy Statement

Trigonon Group B.V. (hereinafter “the Company”), is licensed and regulated by Curaçao Gaming Authority (CGA) to offer remote (online) games on the internet, under the License No. OGL/2024/659/0586. In accordance with the license conditions, The Company has developed a comprehensive Anti-Money Laundering, Counter Terrorism Financing and Counter Proliferation Financing (hereinafter “AML, CTF and CPF”) policy (hereinafter the “Policy”).

Money Laundering (ML) is the process of making funds that originate from criminal activities appear as being originated from a legitimate source. Funding of Terrorism (FT) is the process of using such funds to fund terrorism. We are obliged by law to combat both ML and FT. Our services, since they are widely used, might become a target from criminals to perform ML and FT; by laundering money via online betting games and casinos.

As a responsible gaming enterprise operating in Curaçao, The Company acknowledges the paramount importance of upholding the integrity of our financial systems and preventing the exploitation of our operations for unlawful activities. Our commitment to compliance transcends mere legal requirements; it is a core component of our corporate responsibility and ethical principles.

2. Policy Purpose

The purpose of this Policy is to ensure the Company’s compliance with the relevant legal and regulatory requirements from the authorities in charge of the supervision of AML, CTF and CPF matters for the gaming sector are the CGA and the Curaçao Financial Intelligence Unit (FIU), while simultaneously ensuring the integrity and sustainability of the operations of the Company. The following laws and regulations, as well as any additional regulations issued pursuant to the NOIS, NORUT, the Sanction National Ordinance and the Kingdom Sanction Law, are applicable to the Company:

- Code of Criminal Law (Penal Code) (N.G. 2011, no. 48);
- National Ordinance on Identification of Customers when Rendering Services (NOIS) (N.G. 2017, no. 92), last update June 2024;
- National Ordinance on the Reporting of Unusual Transactions (NORUT) (N.G. 2017, no. 99), last update June 2024;
- Sanctions National Ordinance (N.G. 2014, no. 55);
- Kingdom Sanction Act (N.G. 2016, no. 54);
- National Ordinance of the 20th of December 2024 Containing Rules concerning Games of Chance (National Ordinance on Games of Chance) (PB 2024, no. 157);

- Curaçao Gaming Control Board Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction, last update January 2025.

As a member of the Financial Action Task Force (www.fatf-gafi.org) and of the Caribbean Financial Action Task Force (www.cfatf-gafic.org), Curaçao is meeting international standards by regularly implementing the core standards of these organizations in its national legislation. These laws and standards oblige the Company to adopt risk-based procedures for customer due diligence, monitoring of transactions, and reporting of unusual activities.

By implementing this Policy, the Company aims to ensure that all employees understand and fulfill their legal and regulatory obligations. The Company will apply a risk-based approach to customer due diligence, transaction monitoring, and the reporting of unusual activity. Additionally, this Policy seeks to foster a culture of compliance, transparency, and accountability across all levels of the organization.

From a business perspective, this Policy aims to protect the integrity of the Company's operations by preventing the platform from being exploited by criminal actors. It also seeks to safeguard the Company's reputation with customers, financial institutions, and regulatory authorities. Furthermore, maintaining eligibility for operating licenses and business partnerships is a key objective, as the Company demonstrates compliance with relevant regulations. Finally, this Policy is designed to ensure business continuity by mitigating the legal, financial, and operational risks associated with AML/CTF breaches.

3. Definitions

CFATF means The Caribbean Financial Action Taskforce, an organization of twenty-four (24) states of the Caribbean Basin, Central and South America, which have agreed to implement common countermeasures to address money laundering.

Compliance Officer means A senior officer at management level and independent from the games' operations, responsible for the detection and deterrence of money laundering and terrorist financing.

FATF means The Financial Action Task Force. An independent intergovernmental body, established in 1989 and mandated by its Member Jurisdictions to develop and promote policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction.

FATF Recommendations means A framework of recommendations on policies and measures, issued by the FATF, to combat money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction;

Financial Transactions include the purchase or cashing in of casino chips or tokens, the opening of an account, wire transfers and currency exchanges. Financial transactions do not refer to gambling transactions that include only casino chips or tokens. Amounts wagered and winnings are considered as gambling transactions. Gambling transactions are not considered as financial transactions.

Financing of proliferation (PF) is 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.

FIU means The Financial Intelligence Unit Curaçao, referred to in art. 2 of the NORUT.

Kingdom Sanctions Act means The National Ordinance also known as the “Rijkssanctiewet”, published under N.G. 2016 no. 54.

Money laundering (ML) is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the proceeds appear to have derived from legitimate origins or constitute legitimate assets. Money laundering may generally occur in three stages. Cash first enters the financial system at the "placement" stage, where the cash generated from illegal or criminal activities is converted into monetary instruments, such as money orders or traveler's checks, or deposited into accounts at financial institutions. At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin. At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.

NOIS means National Ordinance on Identification of Clients when rendering Services (Landsverordening identificatie bij dienstverlening, N.G. 2017, no. 92).

NORUT means National Ordinance on the Reporting of Unusual Transactions (Landsverordening Melding Ongebruikelijke Transacties, N.G. 2017, no. 99).

Politically Exposed Persons (PEPs) means: Foreign PEPs are individuals who are or have been entrusted with prominent public functions by a foreign country and the direct family members or close associates of such persons. Examples are: Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials. Domestic PEPs are individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials, and the direct family members or close associates of such persons. Persons who are or have been entrusted with a prominent function by an international organization refers to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions, and the direct family members or close associates of such persons.

Sanctions National Ordinance means The National Ordinance also known as the “Sanctielandsverordening”, published under N.G. 2014 no. 55.

Source of Funds Refers to how the funds for a particular transaction were obtained by the player, like personal savings, pension release, property sales, share sales and dividends, gambling winnings, gifts, compensation from legal rulings.

Source of Wealth is the origin of all the money a person has accumulated over their lifetime, like employment income, inheritances, investments, business ownership interests.

Targeted financial sanctions are measures imposed by governments or international bodies to restrict the financial activities of specific individuals or entities linked to unlawful activities, such as terrorism or money laundering. These sanctions aim to prevent these parties from accessing the financial system. Unlike general sanctions that apply broadly to entire countries, targeted sanctions focus on specific individuals or entities. This approach minimizes the impact on the wider population while addressing particular risks. Targeted financial sanctions apply to

individuals or entities listed on sanctions lists maintained by organizations like the United Nations or the European Union.

Terrorism Financing (TF) refers to the provision of funds or financial support for terrorist acts, individuals, or organizations, and is characterized by the intent to intimidate populations or compel governments and international bodies to act or refrain from acting. Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal either the origin of the funds or their intended use, possibly for criminal purposes. Legitimate sources of funds are a key difference between terrorist financiers and traditional criminal organizations. In addition to charitable donations, legitimate sources include foreign government sponsors, business ownership and personal employment. Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same as or similar to methods used by other criminals to launder funds. Funding for terrorist attacks does not always require large sums of money, such funding could be of cumulative nature over extended periods, and the associated transactions may not be complex.

Unusual transaction A transaction that is considered as such on the basis of certain indicators, pursuant to Article 10 of the NORUT.

(Ultimate) beneficial ownership (UBO) Refers to the natural person(s) who ultimately own(s) or control(s) a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person.

4. Policy Implementation

The Company maintains a comprehensive internal control framework to ensure compliance with applicable laws and regulations related to Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF). The effective implementation of this Policy requires clear responsibilities across all levels of the organization, with defined roles for Senior Management, the Compliance Officer, and employees.

4.1. Senior Management Responsibilities

Senior Management holds overall responsibility for establishing and maintaining a strong culture of compliance. Key responsibilities include:

- Approving the AML/CTF/CPF Policy and ensuring its alignment with regulatory expectations.
- Appointing a qualified Compliance Officer with sufficient authority, independence, and access to all relevant data and personnel.
- Providing adequate resources, including staffing, technology, and training, to support the implementation of the Policy.
- Reviewing and approving the Company's Business Risk Assessment and the annual AML compliance report.
- Overseeing the implementation of corrective actions in response to any identified compliance deficiencies.

4.2. Compliance Officer

The Compliance Officer is appointed at a management level and operates independently from day-to-day operational functions. This individual is responsible for overseeing the design,

implementation, and ongoing monitoring of the AML/CTF/CPF framework. The Compliance Officer also serves as the designated Money Laundering Reporting Officer (MLRO).

Core duties of the Compliance Officer include:

- Ensuring the Company's activities are conducted in accordance with applicable AML/CTF/CPF laws and internal policies.
- Conducting periodic risk assessments and recommending appropriate risk mitigation measures.
- Receiving and reviewing internal reports of unusual transactions and determining whether further reporting to the FIU Curaçao is warranted.
- Maintaining complete records of all internal and external reports, assessments, and training.
- Coordinating and delivering AML training to relevant staff and advising Senior Management on significant compliance developments.

4.3. Employee Conduct And Support

All employees are required to comply with the Company's AML/CTF/CPF obligations and internal procedures. Their responsibilities include remaining vigilant for indicators of potential money laundering or terrorist financing and escalating any concerns to the Compliance Officer through established reporting channels.

4.3.1. Staff Integrity And Screening

The Company applies rigorous pre-employment and ongoing screening procedures to ensure staff integrity and suitability for their roles. This includes verification of identity, background checks, reference verification, and role-specific assessments where necessary. Additional screening measures apply to individuals in sensitive or senior positions.

4.3.2. Training And Awareness

The Company provides AML training tailored to each employee's role and responsibilities.

Training components include:

- Mandatory induction training for all new employees, covering AML/CTF/CPF principles, internal reporting procedures, and regulatory obligations.
- Annual refresher training to maintain awareness and reinforce responsibilities.
- Ad hoc training triggered by regulatory updates, product changes, or identified compliance weaknesses.

The Compliance Officer maintains a training register documenting attendance, content delivered, and testing outcomes where applicable.

5. Risk based Approach (RBA)

Risk-management procedures are applied to control and mitigate higher risk situations. The purpose of the RBA is not to restrict our customers from performing transactions with our business but rather evaluate the risks and when appropriate tackle them in an effective manner

by performing EDD procedures. All customers regardless of their risk level go through the CDD procedures, even if they are marked as low risk customers.

5.1. Business Risk Assessment

To effectively apply the risk-based approach, the Company conducts a preliminary assessment of the risks associated with money laundering and terrorist financing within the organization, and based thereon develops and implements suitable policies, procedures, and controls to manage and mitigate these identified risks, including the present Policy.

The Business Risk Assessment (BRA) framework is a crucial component of The Company's AML, CTF, and CPF compliance program. It provides a systematic, risk-based approach for identifying, assessing, and mitigating money laundering, terrorist financing, and proliferation financing risks within the Company's operations.

The Company performs thorough BRAs, evaluating potential risk factors related to customers, products and services, geographic locations, and delivery channels. Each risk factor is assessed for its likelihood and potential impact. Tailored controls and measures are then implemented to address these risks, including, but not limited to this policy. All findings, evaluations, and mitigation strategies are documented and reported to senior management and relevant regulatory authorities.

BRAs are conducted regularly to maintain an accurate risk profile, with comprehensive assessments performed regularly. Additional assessments may be triggered by significant events, such as the introduction of new products, regulatory changes, or major shifts in the business environment.

1. Risk originating from Customers (target customers)
 - a. Our customers are Non face-to-face customers
 - b. Thus, the risk is HIGH (6-8/10)
2. Risk originating from Service/Product
 - a. We operate a web-based betting platform
 - b. Thus, the risk is HIGH (6-8/10)
3. Risk originating from the Interface (connecting customers with the service)
 - a. The Internet connects our business with our customers and vice versa.
 - b. Thus, the risk is HIGH (6-8/10)
4. Risk originating from Geographical location
 - a. The business can operate in several countries (based on the respective licenses)
 - b. Thus the risk is HIGH (6-8/10)

As it can be observed our business has a HIGH risk based on these 4 factors. Since our customers are not face-to-face, the risk is by default considered to be high and EDD must be applied. We are not accepting cash as a payment method, certain risks are minimised because the payment options we offer to our customers go through verified and reputable payment providers that also apply CDD and EDD procedures. However, this only means that we have a

better chance of identifying ML/FT activities and not that we will solely rely on these services to perform AML/CFT.

5.2. Customer Risk Assessment

Customer Risk Assessment is an essential part of the Company's Anti-Money Laundering (AML) program. It begins when a new customer applies for an account. Based on the information provided, the Company assigns a risk rating (low, medium, or high), which determines the level and frequency of due diligence and monitoring.

The assessment considers the following key areas:

- **Customer Risk:** This includes factors such as the customer's occupation, income pattern, and transaction behavior. Higher risk is assigned to politically exposed persons (PEPs), high spenders, those with inconsistent income sources, or customers using third parties to avoid standard checks.
- **Product and Service Risk:** Certain gaming products or payment methods (e.g., pre-paid cards, virtual assets, peer-to-peer games, or unverified wallets) may carry increased risk due to their potential for misuse.
- **Geographic Risk:** Customers from countries with weak AML enforcement or high corruption levels are considered higher risk. Sources such as FATF and other global risk indices are used to assess this factor.
- **Delivery Channel Risk:** The way services are accessed matters. Online, non-face-to-face channels that may allow anonymity are considered higher risk and are subject to additional controls.

Customers are classified from a scale of low to high risk. This scale is indicated by 1-6. When a customer joins our business we by default give a risk level of 3 which is considered the default risk for new users in our platform. Based on the risk rating:

- **Low-risk customers** may be subject to Simplified Due Diligence (SDD), provided their transactions remain below Cg. 4,000 and no red flags are present.
- **Medium and high-risk customers** require additional information and ongoing monitoring.
- **High-risk or suspicious accounts** are reviewed by compliance staff and may be escalated to the Compliance Officer for further investigation.

This approach ensures that customer risks are properly understood and managed in line with Curaçao AML regulations.

In relation to mitigating the risks, we do not solely perform EDD, but also we apply certain service limitations for customers with high risks.

- Bet limits can be applied (amount)
- Bet delay can be applied (in seconds)
- Customers might be restricted to use certain payment methods of the service
- Customers might be restricted from using certain parts of the service (e.g casino section).

- Customers might not be able to perform transactions at all until EDD checks are completed
- Customers will be reported to the official authorities (FIU) in case that we identify ML/FT activities

6. Customer Acceptance Policy

The Company's Customer Acceptance Policy is formulated in accordance with legal requirements and aligns with the Company's risk appetite as well as the BRA. Therefore, certain categories of individuals are prohibited from being accepted as customers, either by preventing them from registering or by blocking their access to our site, as necessary:

- Individuals under the age of 18.
- Individuals listed on sanctions imposed by UN, EU or OFAC.
- Individuals for whom there are reasonable grounds to suspect involvement in ML/TF/PF or any other form of criminal activity.
- Self-excluded customers who are barred from our websites or included in any national self-exclusion registers as stipulated by licensing conditions.
- Individuals who have submitted documents or information that the Company has reasonable grounds to suspect are fraudulent or falsified.

6.1. Sanctions

The Company is committed to complying with targeted financial sanctions, which require the freezing of funds and assets of individuals and entities identified by the UN and EU as involved in terrorism or proliferation activities.

- **Ongoing Monitoring:** The Company will perform ongoing sanctions screening at key points, including during registration, withdrawal requests, and any changes to personal details or payment methods.
- **Action on True Matches:** If a true match is discovered, the Company will immediately freeze the funds of the affected customer and file a report with the Financial Intelligence Unit (FIU). Services will be terminated upon confirmation of the true match by the supervisory authority, and frozen assets will be held until further instructions are received.

7. Customer Due Diligence

The Company applies a structured and risk-sensitive Customer Due Diligence (CDD) process, beginning at the onboarding stage and continuing throughout the customer relationship. This framework ensures that the Company understands who its customers are, assesses the risk they pose, and applies appropriate verification and monitoring measures in line with Curaçao's AML/CFT requirements under the National Ordinance on Identification when Rendering Services (NOIS) and the National Ordinance on the Reporting of Unusual Transactions (NORUT).

7.1. Customer Identification

In order to use our service, customers are required to register. For registration customers need to provide our business with the following details:

1. Email address
2. Username
3. Password
4. Password confirmation
5. Full name
 - a. First name
 - b. Last name
6. Date of birth
7. Permanent residential address
 - a. Street and street number
 - b. City
 - c. Postal code
 - d. Country
8. Identity reference number
9. Nationality (can be delayed, see SDD section)
10. Identification number (can be delayed, see SDD section)
11. Mobile number (optional)

To complete the first registration phase (before CDD/EDD), the customer needs to verify the provided email or mobile number. A table indicating the customer privileges based on the verification stage is provided below.

Registration phase		Can login	Can play	Can deposit	Can withdraw
1	Registration without email/mobile verification	NO	NO	NO	NO

2	Registration with email/mobile verification but not CDD/EDD	YES	YES, but subject to limited number of bets (verification pending)	YES, but limited amount of deposits or total amount of deposits (verification pending)	NO
3	Registration with full verification and verification	YES	YES	YES, however it is Subject of EDD procedures based on risk	YES, however it is Subject of EDD procedures based on risk

7.1.1. Registration Procedure

1. Customer visits our web-based service to register
2. Customer's country origin (via IP address) is checked to verify that it is within the countries of our operation
3. Customer completes the registration form
4. Customer details are validated with the following rules
 - a. Email must be unique among other registered customers
 - b. Username must be unique among other registered customers
 - c. Identity number must be unique among other registered customers
 - d. Mobile number must be unique among other registered customers
 - e. Passwords must be strong. A minimum of 8-10 characters long phrase that should at least include: 1 uppercase letter, 1 lowercase letter, 1 number and 1 special symbol
 - f. Passwords should not contain the username, email, mobile number, date of birth or identity number of the customer.
 - g. Customer age is calculated based on the given date of birth. Customers should not be minors.
5. If validation is successful, the customer is registered
6. Service sends verification email to the customer's email address
 - a. Once verified customer can login to our application
7. (Optional) Service sends verification SMS to the customer's mobile number

7.2. Verification

7.2.1. Email Verification Process

1. Customer registers with a unique email address
2. A verification email is sent to the email address specified by the customer, including a verification link
3. Customers click on the link to verify their email address

4. Email address of the customer's account is verified

7.2.2. Mobile Verification Process

1. Customer registers with a unique mobile phone
2. A verification message (SMS) is send to the mobile number of the customer, including a 6-digit code (numbers)
3. The customer inputs the code in the mobile verification page of our service
4. Upon successful completion, the mobile of the customer is verified

In most countries, including the country/ies in which this service operates, mobile numbers of a natural person are registered and are associated with the natural person. Verification of the mobile can be considered as a means of CDD, since it is verified by mobile providers.

7.2.3. Customer Due Diligence (CDD)

CDD must be performed:

- When the customer reaches the Cg. 4,000 threshold (cumulatively or per transaction);
- On all withdrawals;
- When doubts arise about prior CDD data;
- When required under NORUT or due to suspicion of ML/TF/PF.

All financial transactions (excluding bonuses or winnings) are counted toward the threshold. Identification and verification must be complete before allowing further transactions.

CDD Measures

- Identity Verification
- IP-check
- Double customer Check

Upon registrations customers are required to provide additional documents so that their identity can be established/verified. CDD is needed to identify potential money laundering activity. The customer's profile needs to be updated constantly so any unusual and suspicious activity can be identified and addressed. The identification details that need to be verified so that the customer can be considered as verified are the following:

Identification details

- Official Full Name
- Date of Birth
- Identity Reference Number
- Permanent Residential Address
- Nationality

Verification Documents

Verification takes place by making reference to official documents, data or information obtained from a reliable and independent source. For the purposes of verification, a reliable and independent source is considered one of the following: a government authority, department or agency, a regulated utility company or a subject person carrying out relevant financial business in Malta or a member state of the EU. This is because such entities would already have verified the identity and characteristics of the person to be verified by our service.

Thus for the verification of full name, date of birth, identification number and nationality, we consult one of the following documents:

- Valid unexpired passport
- Valid unexpired national identity card
- Valid unexpired driving license
- Valid unexpired residence card

For the verification of the residential address, it is performed by making reference to any of the following documents. The documents must not be more than 6 months old, thus any provided document must specify the date it was issued. The customer's full name and address must be present and be accurate in all of the listed documents.

- a utility bill
 - water supply company
 - power supply company
 - heating supply company
 - communication services (landline, mobile phone bills will not be accepted, since the residential address is not considered permanent)
- a statement from a recognised credit institution or bank
- an official conduct certificate
- correspondence from a central or local government authority, department or agency
- a record of a visit to the address by a senior official of the subject person;
- an identification document listed (passport; national identity card; driving license, residence card) where a clear indication of the residential address is provided
- any other government-issued document not mentioned above

7.3. Enhanced Customer Due Diligence (EDD)

Since our customers are not face-to-face and our services are provided over the internet, the ML/FT risk is by default considered to be high and EDD must be applied. However, the extent to which we apply the EDD is determined by the individual customer's risk level and our risk management procedures. All customers are subjects of EDD. When we apply EDD, we essentially apply extra measures to our customers so that we can have more identification details and minimize the risks of ML/FT. Currently, EDD is performed:

- Always for new payment details (deposit/withdraw) debit/credit cards, bank accounts
- Periodically, based on customer risk level

In order to properly address the needs arising from EDD, we apply one or more of the following measures:

- a) Establish the identity of the customer with additional documentation and information
 - i) As provided in section **Verification Documents** (sections in this document)
 - ii) Documents for EDD must be additional to the documents of CDD
 - iii) Documents for EDD that are of the same type (e.g utility bill) with documents obtained for CDD purposes, must be issued from different entities/ service providers
- b) Use supplementary measures to verify the provided documentation
 - i) Certification by legal professional, accountancy professional, a notary or a person undertaking relevant financial business
 - ii) Obtained documents must be a true copy of the original, seen and verified by the certifier, including a photo of the subject customer
 - iii) The certification must include the certifier's signature, profession, contact details and the document's review date
 - iv) Extra attention should be paid to certified documents originating from high-risk jurisdictions
- c) Confirm (certify) the documentation, using a person carrying out relevant business with the subject

7.3.1. Politically Exposed Persons (PEPs)

A PEP is defined as a natural person who is or has been entrusted with prominent public functions. Close family members or persons known to be close associates of such persons (PEPs) are also considered as PEPs in the eyes of the law. Close family members include:

- spouse/partner (recognized by law)
- Children and their spouses
- The parents

PEPs are considered a high risk in regards to ML/FT because of their position which makes them vulnerable to bribery via funds that originate from illegal activities. Based on that, we apply extra EDD measures in relation to PEPs. These are:

- a) Ask for senior management approval (risk management officer)
- b) Establish the source of wealth and funds of the PEP
- c) Enhanced monitoring

To identify PEPs we consult the available PEP lists available in the countries of our operation. In case that the details of a customer potentially show that the subject customer is a public figure or a relative of one, we contact the customer and we apply EDD as described above.

7.4. Monitoring

7.4.1. Ongoing Customer Profile Monitoring

During the periodic review of a customer, The Company verifies and confirms that the CDD information about the client, nature and purpose of the business relationship, and SOF is still accurate and up to date, evaluate if there are external signals (bad press/adverse news, incidents) that could give rise to a change in the business risk profile of the customer and ensure to perform screening against sanctions lists and PEP lists. The periodic review also includes an overall review of the transaction behavior of the client to determine if unusual activities have taken place, for instance in case of transactions which normally would not be expected.

The periodical review of the customer is based on the risk profile of the customer:

- For high-risk customers – once per year;
- For medium risk customers – once every 2 years;
- For low-risk customers – once every 3 years.

7.4.2. Ongoing Transaction Monitoring

The Company performs both real-time monitoring of transactions, as well as post-event monitoring, to ensure that such transactions and activity are consistent with the Company's knowledge of the client and their expected activity. More attention is paid to high amounts, high-risk clients and high-risk jurisdictions.

Particular risk factors will be closely monitored concerning business relationships and transactions, including:

- Gambling or transaction patterns that diverge from what is considered normal or what the customer initially indicated when establishing the business relationship.
- Execution of unusually large transactions by the customer.
- Requests for withdrawals to accounts other than those verified to belong to the customer (such withdrawals are prohibited).
- Requests to transfer gambling accounts or winnings to third parties (such transfers are also prohibited).

8. Reporting of Unusual Transactions

8.1. Reporting Obligations

All unusual activities and transactions, including attempted transactions, are initially reported internally. The officers responsible for transaction monitoring must immediately report any unusual activities to the Compliance Officer upon identification, providing a brief description of the specific mitigating measures taken.

All employees who engage with customers or have access to customer information receive anti-money laundering training. This training prepares them to identify actions by customers that may reasonably raise suspicions of money laundering or terrorism financing. Staff members are expected to recognize and understand any gaming or transaction behaviors that might indicate customer involvement in money laundering or terrorism financing. If they know, suspect, or have reasonable grounds to believe they are dealing with the proceeds of crime, they must submit an Internal Unusual Activity Report to the Compliance Officer (CO) in accordance with the Reporting Procedure. This ensures that the employee's legal obligation to report is fulfilled. Please see [Appendix III](#) for the Report form.

Employees are required to report any unusual activity to the Compliance Officer immediately, but no later than 24 hours after the transaction has been executed, using the Internal Unusual Activity Report form. If a more in-depth investigation is necessary, the Compliance Officer will complete this within ten (10) business days. During this time, the Compliance Officer may request additional information from relevant departments.

If the Compliance Officer concludes that the activity is unusual, a report shall be submitted to the FIU Curaçao regarding any unusual monetary operations or transactions within 48 hours. In any cases whereby the report is made under one of the objective indicators, as defined below, the report must be made to the FIU Curaçao no later than 48 hours after the transaction has been executed.

8.2. Recognition of Unusual Transactions

Staff will be trained to recognize unusual transactions based on customer profiles and specific indicators. Reporting procedures to the compliance officer will be established. In accordance with the FATF Recommendations, the Company and its employees pay particular attention to all complex or unusually large transactions, as well as any unusual transaction patterns that lack a clear economic or legitimate purpose.

The following transactions or intended transactions are deemed unusual:

- a. A transaction, which is reported to the police or judicial authorities in connection with money laundering or the financing of terrorism;
- b. An intended transaction carried out by or for the benefit of a natural person, legal person, group or entity which is on a list compiled by virtue of the Sanctions National Ordinance (N.G. 2014 no. 55);
- c. A transaction amounting to Cg. 5,000.00 or more, regardless of whether this transaction is carried out in cash, via a check or another payment instrument or electronically or in any other non-physical manner. This includes but is not limited to:
 1. A cashless transaction in the amount of Cg. 5,000.00 or more.

2. Accepting or releasing a deposit in the amount of Cg. 5,000.00 or more at the request of the customer;
3. Sale to a customer of chips in the amount of Cg. 5,000.00 or more. "Chips" include but is not limited to tokens and credits.
4. A cash out in the amount of Cg. 5,000.00 or more;
- d. Transactions where there is cause to presume that they can be related to money laundering or terrorist financing.

Please note that indicators (a) to (c) are referred to as "objective indicators", while (d) is referred to as "subjective indicator". While the objective indicators are based on measurable facts and do not require interpretation automatically classifying a transaction as unusual, the subjective criterion involves a more nuanced assessment, considering the context and behavior of the client. For the purposes of reporting unusual transactions under the objective indicators above, it is noted that the threshold of Cg. 5,000.00 resets per game day of the user.

8.3. Prohibition of Disclosure

All reports and investigations must be handled with the highest level of confidentiality in accordance with Article 20 of NORUT. Unauthorized disclosure of information related to unusual activity reports is strictly prohibited and may lead to legal and disciplinary action.

The Company has implemented a system of measures to ensure that employees and representatives who report suspicions of money laundering, terrorist financing, and/or financing of proliferation to the FIU Curaçao are safeguarded from threats or hostile actions by other employees, members of the management body, or customers. Additionally, they are protected from adverse or discriminatory employment actions.

8.4. Record Keeping

The Company keeps all necessary records of customer transactions—both local and international—for at least five (5) years. These records must be detailed enough to show what happened in each transaction, including amounts, currencies, and other key information, in case authorities need them for investigations or legal proceedings.

We also keep all documents collected during customer due diligence (CDD), like ID copies, account files, and correspondence, for at least five (5) years after the customer relationship ends or after a one-time transaction.

All records are stored securely to protect their accuracy and confidentiality. Only authorized staff can access them. We also back up electronic records regularly and keep copies in a secure location to prevent data loss.

When the 5-year period ends, records are destroyed in a way that ensures no unauthorized person can access or recover them.

If required by law, court order, or a regulatory request, the Company will provide any necessary records, including those from CDD or enhanced due diligence (EDD), and will log what was shared and keep a copy.

9. Anti-Money Laundering Compliance Program

9.1. Appointment of a Compliance Officer

A senior compliance officer will be designated, separate from our gaming operations, responsible for overseeing the AML program and ensuring compliance with regulations. Our AML compliance officer will have timely access to customer identification data, transaction records, and other relevant information. This officer will operate independently to ensure robust compliance.

9.1.1. Duties of the Compliance Officer

The compliance officer shall be assigned at least the following responsibilities:

- To design and implement the AML program;
- To verify adherence to local laws and regulations regarding the detection and deterrence of money laundering and terrorist financing;
- To review compliance with the Company's policy and procedures;
- To organize training sessions for the staff on various compliance-related issues;
- To analyze transactions and verify whether any are subject to reporting according to the indicators mentioned in the Ministerial Decree regarding the Indicators for Unusual Transactions;
- To review all internally reported unusual transactions for their completeness and accuracy with other sources;
- To keep records of internally and externally reported unusual transactions;
- To execute closer investigation of unusual transactions if necessary;
- To prepare the external report of unusual transactions;
- To make necessary changes to the AML program;
- To remain informed on the local and international developments on money laundering and terrorist financing and to make suggestions to management for improvements; and
- To prepare periodic information on the Company's efforts against money laundering and financing of terrorism and financing of proliferation.

9.2. Employee Screening and Training Programs

9.2.1. Employee Due Diligence

Employee due diligence is a process employed to screen employees with the objective of identifying and reducing The Company's exposure to the risks associated with money laundering and terrorism financing. These procedures apply not only to the Company's contractual employees, but also to its contractors and subcontractors.

Any employee whose position may enable them to facilitate ML or TF must undergo screening. This requirement applies to prospective employees prior to their hiring for such roles, as well as current employees from time to time. Regular updates and re-evaluations are essential for maintaining an effective compliance program against ML, TF and PF.

To screen both current and potential employees, The Company will:

- Identify the individuals;
- Verify their identity;
- Confirm their employment history, such as through references; and

- Determine their suitability for the position and assess whether they pose any risk to the Company.

Positions that may render an employee vulnerable to collusion with or coercion by criminal organizations should undergo more rigorous checks. The Company must evaluate whether:

- The employee has a criminal record, which may be verified through a police check.
- The employee is or has been subject to regulatory, court, or legal actions.
- The employee has leveraged bankruptcy laws for personal gain.

9.2.2. Training

The Casino provides AML, CTF, and CPF training based on each employee's role and responsibilities. Training covers what staff need to know and do to meet legal and policy requirements. We keep records of all training

- Details on the content of the training programs;
- The names of the staff members who have received the training;
- The date on which the training was provided;
- The results of any testing carried out to measure staff understanding of money laundering and terrorist financing requirements; and
- An ongoing training plan.

Training is updated regularly to reflect changes in laws, regulations, or company policies. Extra training will be given when:

- New rules are introduced
- New products or services change our risk exposure
- A breach happens due to lack of knowledge

9.3. Independent Audit Function

An independent audit function will be established for the annual evaluation of the AML program, ensuring audit personnel are qualified and findings are documented. The audit must include several key assessments, such as:

- Reviewing the Company's AML, CTF and CPF manual.
- Examining customer files.
- Evaluating compliance management.
- Conducting transaction testing.
- Assessing the adequacy of training.
- Ensuring compliance with relevant laws and regulations.
- Evaluating the system's capacity to detect unusual activities.
- Interviewing employees involved in transactions and their supervisors.
- Sampling unusual transactions and reviewing compliance with internal and external policies and reporting requirements.
- Assessing the effectiveness of the record retention system.

The audit shall also evaluate The Company's responsiveness to previous audit findings. All testing scope and results must be documented, with any deficiencies reported to senior management, along with requests for prompt corrective actions.

9.4. Examination by the Curaçao Gaming Authority

The Company shall provide information and documentation regarding its money laundering and terrorist financing policies and procedures to examiners of the CGA during examinations or upon request. The following items must at all times be readily available and accessible:

- The written and approved AML Compliance Program addressing ML/TF/PF.
- Records of the Business Risk Assessment.
- The name and job description of the Compliance Officer responsible for the company's AML policies and procedures.
- Records of reported unusual transactions.
- Records of unusual transactions that required further investigation.
- Records of frozen accounts.
- A schedule of training provided to personnel on ML/TF/PF.
- Assessment reports on the company's policies and procedures regarding money laundering, terrorist financing, and proliferation financing from the internal audit department or an external auditor.
- Customer files, including risk assessments, CDD, customer acceptance, and transaction information.

10. Compliance and Consequences of Non-Compliance

The Casino is fully committed to adhering to all applicable laws and regulations related to Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and sanctions enforcement as established by the jurisdiction of Curacao, aligning with international best practices, including the FATF Recommendations. Compliance with this Policy is mandatory for all employees, officers, agents, and third-party service providers. Non-compliance may expose the organization and individuals to significant legal, regulatory, and reputational risks, including fines or penalties imposed by Curacao's authorities, revocation or suspension of the Casino's gaming license, and potential criminal prosecution for wilful violations.

Additionally, non-compliance can lead to reputational damage, resulting in loss of customer trust, negative media exposure, and strained relationships with financial partners. Operational disruptions may also occur, such as freezing of funds, loss of access to financial systems, and increased scrutiny from regulators.

Employees who violate the AML/CTF Policy may face disciplinary actions, including formal warnings, suspension, or termination for serious or repeated breaches, as well as potential referral to law enforcement. Third-party providers may have their agreements terminated if found non-compliant. All employees must understand and comply with the AML/CTF Policy, participate in mandatory training, and report any unusual behavior or breaches to the Compliance Officer, who will ensure that whistleblower protections are in place.

The Compliance Officer and senior management are responsible for investigating violations, determining appropriate disciplinary actions, and reporting serious breaches to relevant authorities. All enforcement actions are documented and reviewed periodically to improve the compliance program.