

KYC, AML AND CTF POLICY AND PROCEDURES

September 2025

Version:	2.0
Date of Version:	September 2025
Created By:	Ron Brochstein
Confidentiality Level	For External DD purposes

The information presented in this document is privileged confidential information of Sunflower Seed B.V. ("Company") and is also protected subject matter of copyrights owned by Company and of agreements between Company and other parties. Copying, transmission and disclosure of such information can only be done within the strict scope of a governing Company agreement. While all efforts have been made to ensure that the content of this document is accurate at the time of publication, the data upon which this document is based is subject to future change. The information contained in this document is exclusively intended for the individual or entity to which it is delivered. If you are not the intended recipient of this document, you are hereby notified that any review, disclosure, dissemination, distribution or reproduction of this document in any way or act is prohibited.

Table of Contents

1. Document Information	4
2. Approval and Version History	4
3. Definitions.....	5
4. Policy Overview	7
4.1. Introduction	7
4.2. Purpose	7
4.3. Money Laundering.....	8
4.4. Terrorist Financing	9
4.5. Proliferation Financing.....	10
4.6. Targeted Financial Sanctions	10
5. Policy Implementation	10
5.1. Responsibility of the Senior Management	10
5.2. Compliance Officer	11
5.3. Employees	11
5.3.1. Employee Screening	11
5.3.2. Professional Support and Training	12
6. The Risk-Based Approach	12
6.1. Explanation of the Risk-Based Approach	12
6.2. Business Risk Assessment	12
6.3. Technological Developments Risk Assessment	13
7. Customer Risk Assessment.....	13
7.1. Customer Risk	14
7.2. Product and Service Risk	14
7.3. Geographic Risk	14
7.4. Delivery Channel Risk	15
8. Customer Acceptance Policy.....	15
8.1. Prohibited Accounts	15
8.2. Sanctions Screening.....	15
8.3. Politically Exposed Persons (PEPs)	16
9. Customer Due Diligence (CDD)	16
9.1. Customer Identification and Verification	17
9.2. Verification Of Beneficial Ownership	17
9.3. Customer Risk Assessment and Purpose of Relationship	17
9.4. Simplified Due Diligence (SDD)	18
9.5. Timeline for Compliance and Non-Compliant Documents	18

9.6.	Affiliate and PSP Due Diligence	18
10.	<i>Enhanced Due Diligence</i>	19
11.	<i>Ongoing Monitoring</i>	20
11.1.	Player Transaction Monitoring Rules	20
11.2.	AML/CTF Detection and Management.....	21
11.3.	Company Operator Tools	22
12.	<i>Reliance on Third Parties to Perform CDD</i>	22
12.1.	Risk Management	23
12.2.	Identity Verification Processes	24
13.	<i>Reporting of Unusual Transactions</i>	24
13.1.	Recognition of Unusual Transactions	24
13.2.	Internal Reporting	26
13.3.	External Reporting	26
13.4.	Prohibition of Tipping Off	26
13.5.	Record Keeping	26
14.	<i>AML Compliance Program.....Error! Bookmark not defined.</i>	
15.	<i>Consequences of Non-Compliance</i>	28
16.	<i>Related Policies and Procedures</i>	28
17.	<i>Appendix A.</i>	29

1. Document Information

Approval	Board of Directors
Responsible Office	Compliance Officer
Review	Annually
Audience	All Employees, Contractors, and Third Parties This document may be shared under confidentiality restrictions for DD purposes
Effective Date	
Next Review Date	

2. Approval and Version History

Date	Version	Summary Changes	Approved by Management
January 2023	1.0	Policy implementation	
September 2025	2.0	Policy updates for alignment with CGA AML Regulations	 ----- Gouloud Hammond f/obo Guardian Corporation Curacao B.V. Corporate Director

3. Definitions

"CGA"	Curaçao Gaming Authority
"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.
The "Company"	means Sunflower Seed B.V. (company number 157063, registered address Kaya Richard J. Beaujon Z/N, Willemstad, Curaçao) which is a holder of license number OGL/2024/198/0418 from the CGA.
"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 traveller'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 Overview

4.1. Introduction

The Company is licensed and regulated by Curaçao Gaming Authority (CGA) to offer remote (online) games of chance, under License No. OGL/2024/198/0418. In accordance with applicable legislation and its 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").

Due to continual growth in the use of electronic trade and online transactions, online money laundering and online fraudulent behaviour is constantly on the rise. Company implements and employs policies and procedures to mitigate the risks involved in such activities. To ensure that Company is not used to launder proceeds from criminal activities or questionable sources, Company recognizes the need to have in place up-to-date systems and procedures to combat money laundering and terrorist financing. These systems and procedures are designed to deter criminals and to protect the Company, those employed by Company and its business reputation.

In addition, under most jurisdictional requirements gambling Operators have a responsibility to keep financial crime out of gambling, and with remote environments, where the financial integrity of the transaction can be ascertained, there are additional responsibilities to protect against money laundering.

4.2. Purpose

This document's purpose is to describe Company's anti-money laundering protections, procedures and tools used to monitor and protect Company against Money Laundering ("ML"), Terrorism Financing ("TF") and Proliferation Financing ("PF").

This document outlines the obligations that Company has as an Operator and in addition, further outlines the policies and procedures for Company in line with the general company obligations including:

- To assist in understanding the obligations and responsibilities that arise from Anti-money Laundering (AML) and Counter Terrorist Financing (CTF) legislation. This is related to both Company as a registered company and a licensed Operator .
- To assist in the implementation of, and compliance with, Anti Money Laundering and Counter Terrorist Financing Compliance Policies. This relates to Company as a licensed Operator.
- To protect the directors, officers and employees of Company and the reputation of Company and its brands. This is related to Company as an incorporated entity.

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;
- National Decree penalties and fines reporting unusual transactions (N.G. 2021, no. 69) as amended by PB 2023, no. 6.;
- Ministerial Decree with general operation of November 11, 2015, laying down the indicators, as mentioned in article 10 of the National Ordinance on the Reporting of Unusual Transactions (Regulation Indicators Unusual Transactions) (N.G. 2015, no. 73);
- Sanctions National Ordinance (N.G. 2014, no. 55);
- Kingdom Sanction Act (N.G. 2016, no. 54);
- National Decree entering into force of Kingdom Sanction Law (N.G. 2017, no. 2);
- National Ordinance extension of validity sanction decrees 2018 (N.G. 2018, no. 34);
- 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 fulfil 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 and CPF breaches.

4.3. Money Laundering

Money Laundering is the process whereby a criminal may seek to conceal the true origin and ownership of the proceeds in order to give the impression that these proceeds originated from a legitimate source. There are essentially three stages in Money Laundering:

- **Placement** – The physical disposal of criminal proceeds where the money launderer attempts to place cash into a legitimate financial system.
- **Layering** – The separation of criminal proceeds from their source by the creation of "layers" or a sequence of transactions designed to disguise the audit trail and provide the appearance of legitimacy.
- **Integration** – The conversion of the criminal proceeds, for example, into real estate, property or investments, so that they appear to be legitimate funds or assets.

These stages usually occur in sequence, but they may often overlap. The remote gambling industry is most likely to be exposed to the "layering" stage of money laundering.

Primary judicial AML offences include the following:

- Concealing, disguising, converting or transferring criminal property or removing it from the jurisdiction.
- Entering into arrangements in which a person knows or suspects will facilitate the acquisition, retention use or possession of, "criminal property" by or on behalf of another person.
- Acquiring, using or having possession of an undervalued criminal property.

Lack of notification to the relevant authorities are also an offence, such as:

- Failing to report to the MLRO when an employee knows or suspects, or the employee has reasonable grounds for knowing or suspecting that another person is engaged in Money Laundering. This includes potential and new customers where knowledge is acquired or there is suspicion, the employee must still report the knowledge or suspicion, even if a decision is made not to allow the customer to open an account.
- Disclosing that a money laundering disclosure has been made to the authorities or that an investigation is being contemplated or is being carried out, where the disclosure of that information is likely to prejudice an investigation (known as "tipping off").
- Failing to establish adequate policies and procedures to identify and prevent money laundering.

4.4. Terrorist Financing

In an attempt to combat terrorism, authorities target the funds that finance this activity. Where money laundering is the process where cash raised from criminal activities is made to look legitimate for re-integration into the financial system, Terrorism Financing focuses on the use of the 'laundered' funds. As with other high-volume industries where multiple transactions are carried out every hour and every day, terrorist organizations may attempt to make use of the e-Gambling industry to assist in disguising the source and intended use of these funds.

The following is a non-exhaustive list of terrorism financing offences:

- To be involved in fundraising if an employee has knowledge or reasonable cause to suspect that the money or other property raised may be used for terrorist purposes.
- To use or possess money or other property for terrorist purposes, including when the employee has reasonable cause to suspect they may be used for these purposes.
- To become involved in an arrangement which makes money or other property available to another person, if the employee knows, or has reasonable cause to suspect it may be used for terrorist purposes.
- To enter into or become concerned in an arrangement facilitating the retention or control of money or other property likely to be used for the purposes of terrorism (terrorist property) by, or on behalf of, another person including, but not limited to the following ways:
 - By concealment.
 - By removal from the jurisdiction.
 - By transfer to nominees.

4.5. Proliferation Financing

Financing of proliferation (FP) involves providing funds for the creation, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling, or use of nuclear, chemical, or biological weapons, along with their delivery systems and related materials.

4.6. Targeted Financial Sanctions

We are committed to complying with targeted financial sanctions, which require the freezing of funds and assets of individuals and entities identified by the United Nations (UN) and European Union (EU) as being involved in terrorism or proliferation activities. Mechanisms are established to ensure compliance with these sanctions. This includes, but is not limited to, the following:

- The Company shall comply with relevant sanctions decrees and regulations and monitor for any and all amendments thereof, and implement these without undue delay.
- The Company shall perform perpetual sanctions screening on customers and also perform trigger-based sanctions screening of customers at least in the following scenarios:
 - At the moment of registration;
 - At the moment of withdrawal request;
 - At the moment of any request for change of personal details or payment methods.

In the event that a true match is discovered, the Company shall immediately proceed with freezing the funds of the particular customer(s), in accordance with the Sanctions Ordinance, and shall immediately file a report with the Financial Intelligence Unit (FIU). Once the true match is confirmed by the supervisory authority, the Company shall terminate services and keep the frozen assets until further instruction from the supervisory authority.

5. Policy Implementation

The Company internal controls are a set of policies and procedures aimed at securing the efficient and compliant business within the Company and provision of the safe and fair gambling environment for the customers.

All Company directors, officers and employees are individually responsible for complying with the requirements of this policy. Directors, officers and others in management or leadership roles must lead by example, showing commitment to compliance and promoting awareness. All employees will be familiar with this manual and with their duties in relation to this manual. Where the Company engages the services of third parties to assist in Company's compliance with AML and CTF laws, the responsibility for compliance remains with Company.

Failure to comply with Company policy is a disciplinary offence which could result in disciplinary action.

5.1. Responsibility of the Senior Management

The Senior Management is responsible for:

- setting and approving the general principles underlying the Policy for Prevention and Combatting of Money Laundering and Terrorist Financing
- appointing Compliance Officer and communicating to them the internal policies
- defining the duties and responsibilities of the Compliance Officer
- ensuring that effective and sufficient systems and controls are in place to enable compliance with all rules and regulations
- ensuring that the Compliance Officer have completed and timely access to all data required to effectively undertake their duties including, but not restricted to, data

concerning customer identity, transaction documentation and other relevant information maintained

- ensuring that all employees are aware to whom they have to report any information concerning unusual transactions
- ensuring that the Compliance Officer have sufficient resources including competent staff and technological equipment
- assessing and approving the annual report and taking appropriate actions to remedy any weaknesses and/or deficiencies identified in the annual report.

5.2. Compliance Officer

The Company has appointed a Compliance Officer to lead the AML Compliance program. The Compliance Officer has working knowledge of the Company's business environment, risks inherent to the Company's business model and AML, CTF and CPF provisions as stipulated in the Regulations as amended.

The Compliance Officer is responsible for the following:

- Review and apply the provisions of AML/CTF regulations.
- Engage in and maintain the Risk Committee.
- Promoting, supervising and coordinating compliance with this policy document.
- The focal point within Company for overseeing all activity relating to AML/CTF issues.
- Investigate all reports of suspicious transactions sent and where required, report to the relevant authorities.
- Ensure relevant staff have adequate resource training to effectively contribute to the AML programme.
- Conduct an assessment of Company's AML and CTF risks on a regular on-going basis. The risk assessment will consider risks associated with customer profiles, payment methods, jurisdictions and products.
- Review this manual to ensure its accuracy and compliance with regulatory requirements.

5.3. Employees

5.3.1. Employee Screening

The Company recognizes that employees can pose an AML/CTF risk, through the potential for collusion with customers or other third parties, dishonest manipulation of records or processes, or simply through failure to correctly follow Company's AML and CTF policies and procedures.

To mitigate the risks posed by employees Company has implemented the following screening methods:

- Employees are subject to an employee due diligence screening process prior to commencement of their employment including:
 - A copy of a birth certificate, identity card (where applicable) or official document is required to verify that the employee is over the age of 18 years.
 - Address verification
 - Reference checks.
 - Through the police, check that an employee has not been, or is not involved in any illegal activities such as fraud, money laundering, or organized crime.
- Employees are prevented from holding accounts with Company. Screening is conducted prior to commencement of employment to ensure that no accounts are held, and any found are closed.

5.3.2. Professional Support and Training

All relevant Company personnel (and/or third parties) are required to undergo anti-money laundering training at least once a year. Furthermore, this course must be completed by all new staff within 4 months of joining the Company. Staff must get 80% or over to pass and if they do not, they must retake the test.

In addition:

- Board members received Face-to-face training.
- The Compliance Officer receives direct training throughout the year by attending conferences, doing webinars and conferences and training.

Training components include:

- Mandatory induction training for all new employees, covering AML, CTF and 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.

Relevant personnel include the employees responsible for completing customer due diligence measures as well as all Support staff.

Relevant personnel will be required to show that they have understood the requirements of the Company's AML and CTF Policy and Manual. This will be assessed by a short competency test following each training session. The Compliance Officer maintains a training register documenting attendance, content delivered, and testing outcomes where applicable.

6. The Risk-Based Approach

6.1. Explanation of the Risk-Based Approach

The Company adopts a risk-based approach in our AML compliance program. When developing its AML compliance program, the Company assesses risks in such a way that higher risks necessitate more robust measures to mitigate them. Conversely, for lower-risk scenarios, the Company may employ simplified measures.

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 Company shall continuously monitor and enhance the effectiveness of these policies, procedures, and controls, ensuring that it maintains thorough documentation of its risk assessments, detailing all actions taken and the rationale behind them. The Company shall also assess and manage risks associated with emerging technologies and new gaming products that may facilitate ML/TF/PF activities.

6.2. Business Risk Assessment

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. 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. The Board of Directors shall formally approve the BRA and risk appetite.

6.3. Technological Developments Risk Assessment

In line with the risk-based approach the Company shall conduct a Technological Developments Risk Assessment in order to mitigate any ML, TF and PF risks. The following circumstances should result in an assessment being performed:

- The development of a new product;
- A new delivery mechanism;
- A new business practice emerges, in particular every time money and technology come together in a new way, whether that is a new payment channel, a new way to transfer money between services or a change in the payment infrastructure offered by technological developments, and
- A new technology is used to deliver new or old services.

When conducting a Technological Risk Assessment, the following must be addressed:

- Anonymity Risk: Does the new technology increase the ability for customers to remain anonymous?
- Cross-Border Exposure: Does it facilitate international payments, P2P transfers, or multi-jurisdiction access?
- Licensing/Regulation: Are third-party providers (e.g., e-wallets) regulated in reputable jurisdictions?
- Transaction Traceability: Can the Company maintain a clear audit trail for every transaction?
- Volume and Velocity Risk: Can the product allow rapid/frequent transactions that might facilitate layering?
- Integration with Monitoring: Can the existing AML software capture and analyse transactions from the new channel?
- Contingency & Response: If misuse is detected, can the product be paused or suspended immediately?
- Periodic Re-assessment: Review the risk at launch, at a specified frequency, and annually thereafter.

7. Customer Risk Assessment

The Customer Risk Assessment (CRA) will assess the particular risks the casino will be exposed to when providing its services or products to customers. The information collected to draw up the CRA will formulate the customer's risk profile. On the basis of the CRA, the proper level of CDD can then be applied.

The risk assessment process considers the following factors:

7.1. Customer Risk

This involves assessing the customer's background, occupation, and transaction patterns. High-risk customers, such as politically exposed persons (PEPs) and those from high-risk jurisdictions, receive particular scrutiny. Categories of customers whose activities indicate a higher risk include:

- Customers who have multiple sources of income;
- Customers with irregular income streams;
- PEPs;
- High spenders (money can be derived from illegal activities);
- Disproportionate spenders (inconsistent with casino's information about customer's known source of income/assets);
- Casual customers like locals/tourists, especially when spending pattern changes;
- Improper use of third parties, criminals use third parties to gamble to break up large amount of cash, to buy chips or to cash out on behalf of others to avoid CDD measures;
- Multiple casino player rating accounts to hinder a casino to track their gambling activities;
- Unknown customers (redeeming large amounts of chips);
- Junkets (junket operators monitor player activity and issues and collect credit).

7.2. Product and Service Risk

This factor evaluates the risks associated with the products and services offered. The following products and services are considered to be at higher risk of criminal exploitation. This includes gaming products or services where customers can influence game outcomes, either on their own or in collaboration with others. Additionally, certain payment methods used by customers and accepted by casinos are seen as riskier for ML and TF. The following is a non-exhaustive list of high-risk factors:

- Anonymous payment methods: This includes pre-paid cards and virtual assets.
- Casino account usage: These accounts should only be used for gambling, not for depositing and withdrawing funds without playing or with minimal play.
- Specific game types: Games like roulette and craps, where bets are made even.
- Peer-to-peer gaming.
- Third-party accounts: Customers using accounts or cards that belong to someone else.
- Fund transfers: Moving money from one gaming account to another.
- Financial services: This includes services like credit markers, currency exchange, and check cashing.
- Multiple accounts or wallets: An internet operator might control several websites.
- Changes to financial accounts: Adjustments made to fund casino accounts.
- Identity fraud: Stolen financial account details used on websites, including stolen identities used to open financial accounts that are then used for gambling.
- Pre-paid card funding: Using cash to load a pre-paid card carries similar risks as cash transactions.
- Games with multiple operators: For example, poker platforms shared by different operators.
- Electronic wallets: Not all e-wallets are licensed in trustworthy countries, and some accept cash deposits. Moreover, e-wallets that only accept funds from financial accounts may not show the transaction to the online casino, which could help dishonest customers hide their gambling activities.

7.3. Geographic Risk

This assessment considers the geographic location of the customer and the transaction, with countries that have weak AML/CFT regulations or high levels of corruption being deemed higher risk. The nationality, residence and place of birth of the player have to be taken into account as these might be indicative of a heightened geographical risk. The Company takes into account the following

sources of information produced by the FATF and other well-known non-governmental bodies (not limited):

- Countries on the FATF list of High - Risk Jurisdictions subject to a Call for Action;
- Countries on the FATF list of Jurisdictions under Increased Monitoring;
- 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 (INCSR);
- 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 have terrorist organizations operating within them;
- Countries on the Corruption Perception Index compiled by Transparency International.

The Company consistently monitors updates to the lists above and adjusts its CDD process to reflect relevant changes.

7.4. Delivery Channel Risk

This factor looks at the risks associated with the methods used to establish a business relationship or through which transactions are carried out. The Company considers the increased risk of ML/TF of the use of channels that favor anonymity and interactions on a non-face-to-face basis and, to the extent possible, shall take all reasonable measures to address and mitigate said risks.

8. Customer Acceptance Policy

8.1. Prohibited Accounts

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:

- Legal persons.
- 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.
- Politically Exposed Persons (PEPs).
- 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.
- Customers for whom an elevated risk level in their profile has led the Company to terminate the customer relationship for any reason.

8.2. Sanctions Screening

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.

8.3. Politically Exposed Persons (PEPs)

Immediately upon registration, searches are made against Politically Exposed Persons (PEP), international sanctions and enforcement lists.

Where a potential or existing customer is identified as a PEP or as being on a sanctions list, the individual will be declined as a customer.

Where a customer is identified as being on a sanctions list, their account will be closed immediately by the MLRO.

A PEP is an individual who has been entrusted within the last year with one of the following prominent functions by a state or an international body:

- Heads of state, heads of government, ministers and deputy or assistant ministers.
- Members of parliament.
- Members of supreme courts, of constitutional courts or of other high-level judicial bodies whose decisions are not generally subject to further appeal, except in exceptional circumstances.
- Members of courts of auditors or of the boards of central banks.
- Ambassadors and charge d'affaire and high-ranking officers in the armed forces.
- Members of the administrative, management or supervisory bodies of state-owned enterprises.
- A PEP may also be an executive director, senior officer, trustee, partner, guardian or other individual who has executive or effective control of the customer.

In addition to the primary PEPs listed above, a PEP also includes:

- Family members of a PEP including spouse, partner, children and their spouses or partners, and parents.
- Known close associates of a PEP including persons with whom joint beneficial ownership of a legal entity or legal arrangement is held, with whom there are close business relationships, or who is a sole beneficial owner of a legal entity or arrangement set up by the primary PEP.
- For corporate customers, the situation where a "beneficial owner" of the client is a PEP.

Note: Company policy does not permit PEPs or incorporated entities being registered as customers.

9. Customer Due Diligence (CDD)

The best protection against abuse by money launderers is to know the customer. Customer Due Diligence (CDD) involves finding out who the customers or potential customers are. The identity of the customer with which the Company will engage commercially, is established beyond doubt through the collection of information from the Customer (at registration) and verification of such information through independent means by collecting identification documents and proof of address. The collected documents are reviewed by trained personnel tasked with verifying their authenticity. The Information collected from said documents are transmitted in the form of a query to external service providers in order to confirm the validity of the information.

Note: Company has decided, as a matter of principle, to refrain from accepting Legal Persons as

Company customers and therefore does not receive any funds from incorporated entities.

The Company has an obligation to undertake CDD measures when:

- A customer deposits or stakes €2,000 or makes cumulative deposits or stakes of €2,000.
- A customer withdraws €2,000 or makes cumulative withdrawals of €2,000.
- Any knowledge, suspicion or cause to suspect that a customer is engaged in money laundering or terrorist financing; or
- the Company has doubts about the veracity or adequacy of previously obtained customer identification data.

The CDD measures to be taken are as follows:

- Identifying the player and verifying that customer's identity using reliable, independent source documents, data or information;
- Identifying the beneficial owner and taking reasonable measures to verify the identity of the beneficial owner, such that the casino is satisfied that it knows who the beneficial owner is. For legal persons and legal arrangements this should include understanding the ownership and control structure of the customer;
- Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship;
- Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the casino's knowledge of the player, its business and risk profile, including, where necessary, the source of funds.

9.1. Customer Identification and Verification

The Company's CDD procedures require prospective customers to create a full profile at point of registration. Mandatory information required at registration stage includes:

- Full name;
- Date of birth;
- Permanent residential address;
- Unique and verified email address;
- Phone number;
- Unique nickname; and
- Password.

For the process for Identity Verification, see below Identity Verification Processes.

9.2. Verification Of Beneficial Ownership

Customers must confirm they act on their own behalf. The Company monitors for indications of third-party control. The following safeguards apply:

- Payment method verification: deposits and withdrawals must be made using accounts in the customer's name.
- Monitoring for proxy activity or suspicious behaviour.
- Immediate verification upon withdrawal requests or Cg. 4,000 thresholds.

9.3. Customer Risk Assessment and Purpose of Relationship

Each customer is assigned a risk rating based on:

- Jurisdiction of residence;
- PEP or sanctions status;
- Payment method used;
- Anticipated transaction volumes and types.

The customer must provide their occupation and estimated annual income. This information is verified proportionally to the assessed risk. For High-Risk customers, supporting documentation (e.g., payslips, bank statements, tax returns) is required.

9.4. Simplified Due Diligence (SDD)

SDD may be applied only where:

- The customer is classified as low risk;
- No suspicion of ML/TF exists;
- No indicators of PEP status or high-risk jurisdiction are present;
- The total transaction value is below €2,000.

Under SDD:

- Basic identification is collected;
- Verification may be delayed until specific thresholds are met;
- Monitoring is tailored based on risk, and must still detect unusual activity.

If risk increases or suspicious behaviour arises, SDD must be upgraded to CDD or EDD.

9.5. Timeline for Compliance and Non-Compliant Documents

If the customer cannot provide compliant documents within thirty (30) days from the moment the Cg. 4,000 threshold is reached, the Company shall terminate the relationship with the customer and consider filing an Unusual Activity Report with the FIU, provided that a presumption of ML or TF exists.

During the CDD process, customers may continue to access their accounts while the Company gathers the necessary information. However, if a deposit reaches the Cg. 4,000 thresholds, the customer will be prohibited from further deposits or withdrawals, although they may continue to play with their existing balance. Conversely, if the threshold is reached due to a withdrawal request, the account will be completely frozen, halting all gameplay.

If a document submitted by a (potential) customer does not meet the verification standards, the designated staff member must immediately flag it for further examination. The initial review should be thorough to pinpoint the specific reasons for non-compliance. Once a non-compliant document is identified, the customer must be informed without delay.

All actions taken in response to non-compliant documents shall be carefully recorded. This includes the initial identification of the issue, communications with the customer, any escalations, and the final outcome. Comprehensive records should be maintained in the customer's file to ensure a complete audit trail.

9.6. Affiliate and PSP Due Diligence

Before engaging any affiliate or marketing partner, the Company shall:

- Conduct regular due diligence to verify ownership, location, representation and regulatory background.
- Screen all affiliates and their beneficial owners and representatives against PEP, sanctions and adverse media databases.
- Ensure affiliates are not operating from, or targeting, FATF high-risk or sanctioned jurisdictions.

Payment Service Provider (PSP) oversight includes:

- Conduct initial and periodic due diligence on all PSPs, confirming regulatory licensing and AML adherence.
- Ensure PSPs provide transaction reporting compatible with the Company's monitoring tools.
- Annual risk reviews to confirm PSPs remain compliant and are not processing payments from prohibited jurisdictions.

All affiliate agreements shall contain:

- A prohibition on marketing in prohibited jurisdictions;
- A requirement to adhere to AML, CTF and CPF standards aligned with the Company's risk appetite;
- A right to audit or request KYC evidence from affiliates.

10. Enhanced Due Diligence

Enhanced Due Diligence (EDD) is required when something is detected that requires additional scrutiny. The Company shall implement EDD measures for customers identified as higher risk, with actions tailored to the specific risks identified during the assessment process. These measures aim to intensify monitoring of the business relationship to detect any unusual or suspicious transactions or activities. EDD is required in situations where the risk of ML, TF or PF is heightened.

In any case, the following scenarios are subject to EDD:

- *Residents of High-Risk Geographic Areas:* Customers residing in jurisdictions associated with higher levels of corruption or inadequate AML, CTF, and CPF regulations.
- *Anonymity-Favouring Products or Transactions:* Services or products that allow for a higher degree of anonymity, potentially facilitating illicit activities.
- *New Products and Business Practices:* The introduction of new services, technologies, or delivery mechanisms that may present unforeseen risks.

When EDD is triggered, the first stage of review is performed by the Compliance Officer who conducts an extensive investigation into the issue and the risk factor attached to the issue. If the Compliance Officer deems it necessary, the query is sent to middle management for review and resolution. If the issue still remains unresolved, it is escalated to the senior for final resolution.

EDD may include additional checks on the customer's identity and background using open-source research resources, government watch lists, sanctions lists, and other third party resources and may include additional requests for information from the customer, in appropriate circumstances.

The measures applied during EDD must align with the identified risks and may include, but are not limited to:

- **Additional Customer Information:** Collect comprehensive information about the customer, including occupation, previous addresses, and relevant data from public databases and online resources.
- **Clarification of Business Relationship Intent:** Obtain further information regarding the intended nature of the business relationship to better understand the customer's gaming habits and expectations.
- **Source of Funds and Wealth (SOF/SOW):** Gather detailed information on the source of funds or wealth for the player. Examples include:
 - Personal savings
 - Employment income
 - Pension releases
 - Share sales and dividends
 - Property sales

- Gambling winnings
- Inheritances and gifts
- Compensation from legal rulings

In higher-risk situations, The Company will periodically request SOF information, even if there has been no change in the customer's activity pattern. This ongoing diligence is essential for proactively addressing any potential concerns.

- Transaction Purpose: Ask for information regarding the reasons for intended or performed transactions to ascertain their legitimacy and ensure they align with the customer's profile.
- Senior Management Approval: Require approval from senior management before commencing or continuing the business relationship with higher-risk customers.
- Enhanced Monitoring: Implement increased scrutiny of the business relationship, which may involve more frequent reviews of transactions and account activities.
- Account Verification for Initial Payments: Require that the initial payment is made through an account in the customer's name with a bank that adheres to similar CDD standards.

If CDD cannot be completed satisfactorily, the customer's registration must be declined or, in the case of existing customers, further activity must be suspended, including the withholding of payment of winnings or remaining deposits, and the business relationship with the customer must be terminated. A suspicious activity report may also be required to be made to the relevant authorities.

11. Ongoing Monitoring

The initial satisfactory identification of a new customer and knowledge of the client's source of funds is not, of itself, sufficient to protect the Company from exposure to money laundering and terrorist financing risk. There is a continuing duty to conduct ongoing monitoring of customer relationships and to be vigilant with regard to money laundering and terrorist financing at all times and to report any suspect transactions or circumstances.

Business relationships must be subject to ongoing monitoring on a risk-sensitive and appropriate basis. Ongoing monitoring includes:

- Scrutiny of transactions undertaken throughout the course of the relationship (including the source of funds) to ensure that the transactions are consistent with Company's knowledge of the customer, its activities and risk profile. Particular attention is placed on transactions that are complex, large and unusual or part of an unusual pattern.
- Updating the documents, data and other information obtained for the purpose of identifying the customer.

11.1. Player Transaction Monitoring Rules

Once the rules have been configured by the Company, these rules run automatically against the defined players or groups of players, and can be used to monitor behaviours and transactions in real time.

The rules generate alerts for handling. Rules matching alerts are always monitored through a real time reporting and statistics system.

The rules can be configured to take automatic actions or to send a flag to the Company to raise an alert that a rule has been triggered. The rule engine allows the Company to define specific rules tailored exactly for its business processes and regulatory requirements.

The rules can be triggered at any time of a player's lifespan or at any event during their lifespan.

The rules can pro-actively trigger a wide set of actions/sanctions that have an immediate future effect on the player's account (freeze account, cancel transaction, and so on.)

11.2. AML/CTF Detection and Management

The Company applies advanced tight fraud detection and management tools with applications to safeguard against collusion and other types of fraudulent player behaviour.

Major solutions include:

- Deposit limits and players risk profile tools.
- Fraud automated rules for fraud detection, automated functionalities and flagging.
- Fraud case handling and analysis.
- Duplicate activity monitoring and management. Bad data and player bans.
- Fraud detection and identity theft monitoring for general patterns and suspicious behaviour.
- Configurable Reports including statistic interfaces, report creation and viewer defined reports.
- Blocking/restriction features for bad data, serial blocking, freezing players, and so on.
- Payments procedures for payment method configurations, withdrawal process, audit procedures.
- Duplicate Account Mechanism which is an essential tool during signup stage. During the Signup stage a search can be made for:
 - Duplicate accounts – Most online casinos are suspicious of duplicate accounts which are considered to be a sign of possible fraudulent behaviour, similar to bonus seeking or not complying with deposit limits. When a new account is found to be a duplicate, one of the player's accounts is automatically disabled. The decision as to which account is disabled depends on several factors, such as the period of inactivity and net loss.
 - Related accounts – These accounts are created when Company operates several casinos from one backend system with the same backend scripts and Casino Admin controlling all accounts. Related accounts are generally permitted.
 - When a new account is created, duplicate or related accounts are checked for fraudulent activity. The following events may be detected:
 - Previous fraudulent credit card activity, such as chargebacks or refunds.
 - Previous fraudulent non-credit card activity, such as returned checks.
 - Bonus seeking.
 - Blocked serial numbers for fraudulent reasons, such as chargeback risks.
 - Suspicious information, for example the same credit card used by different people or with fake details.
- Live Alerts and Automated Rules – Actions taken by the player that initiate a rule including:
 - Sign Up.
- Payment method registration.
 - Deposit.
 - Withdrawal.

These rules are configured by outlining the trigger, the condition, the exception to the rule, the action to be taken and the communication to be made to player or Operator when rule is triggered. For example, at signup, all customers from a certain jurisdiction, will have ID verification triggered. When this is triggered, the player receives an automatic email requesting ID.

- Deposit Limits
 - When an account is opened, the Admin automatically applies deposit limits based on the player's country and other customizable rules. These limits can be updated for each player according to deposit checks and data accumulated during the player's lifecycle.
 - Deposit limits are based on a matrix of default limits multiplied by different risk factors (coefficients) to define the effective deposit limits for the player, based on:
 - Risk profile.
 - Age trust factor.

- Currency rate.
- Serial Number Mechanism

Most online gaming Operators enable their players to open only one account per device. However, there are exceptions. This could be for members of the same household where each member has their own account on a shared computer.

When a player downloads a client (whether to create a new account or use an old one) or accesses the flash client from casino site, the Company gaming software places a serial code in the player's computer registry. This number is also displayed in the Admin in the player's Users Info page Signup Information section.

If a player attempts creating additional accounts, the Admin reads the serial number, and according to the Operator's policy, enables or blocks the player from completing this action.
- Country/IP block
 - This feature allows countries to be blocked based on the IP.
 - If the Company decides not to block the country at registration, this can be done at other points during a player's interaction with the system, such as but not limited to, making deposits or placing bets.
 - If the Company wishes it may enable a player from the certain country to register and operate an account with actions such as making deposits and placing bets, while still implementing various rules and triggers based on a specific country, and can flag these players as high, medium or low risk. This risk flag can trigger an automatic action occurring such as ID verification being required, and an email sent or notification sent to the Company to review this player.

11.3. Company Operator Tools

The Company is provided with configurable tools enabling the Company to put in place triggers and rules based on risk profiles. Once triggered, these rules can either result in an alert or continue with a predetermined action based on the configurations, for example freezing a player account. All tools in the system can be configured to meet various regulatory jurisdictions including but not limited to Malta, Alderney and UK.

Enhanced search parameters can be set to single out different aspects of fraud set by the Company or based on regulation dictate, enabling the Company to mitigate such behaviour. This refers both to money laundering and terrorism financing, as well as other fraudulent behaviours, such as fraudulent behaviour deriving from a specific country of origin, stolen identity or stolen credit cards.

These tools may be used in AML policy and procedures and include:

- Verification Processes
- Automation Rules
- Fraud Detection and Management
- Risk Management

These tools allow compliance with regulatory requirements and provide various configurations ensuring funds are remitted to the same account from which funds originated, or where deposits and withdrawals can be flagged, if the total accumulation of withdrawals equals or exceeds a certain sum in a defined period of time. In addition to other tools used to detect other various suspicious transactions and behaviours.

12. Reliance on Third Parties to Perform CDD

12.1. Risk Management

Company utilizes the services of a third-party risk management team. This team consists of professional data analysts and fraud and risk agents. The team is dedicated to risk management and as it provides services independently to multiple companies/operators and brands, Company benefits from knowledge and experience gathered in combating fraud in or perpetrated against other industry leaders.

A team's accumulated experience enables it to develop a more comprehensive knowledge base providing the team with the ability to constantly upgrade forecasting abilities, which in turn increases the chances of preventing and fighting fraudulent activities.

The third-party risk management team is responsible for preventing and handling all incidents of suspected and fraudulent behaviour. With the aim of detecting fraud in its beginning stages, the team's activities are designed to follow the player's lifecycle. Potential risks are estimated at each stage, and when required, preventative measures are taken to minimize the financial risks.

While the team structure may depend on operational volume, interaction with payment processing departments and number of department employees, fraud departments usually have the following tasks:

- Review and verification of player documentation.
- Preventing and handling players who abuse the system when engaged in gaming activity. For example, bonus seekers, card counters and poker colluders.
- Dealing with chargebacks and Automated Clearing House (ACH) issues, ideally made before the chargeback is initiated.
- Handling disputes with players.

Services that the third-party risk management team perform:

- Configuring and monitoring fraud rules.
- Analysing current and new players' deposits and withdrawals.
- Identifying suspicious behaviour, fraud rings and behaviour patterns.
- Applying preventive steps and sanctions.
- Following regulatory requirements, create strict procedures to deal with anti-money laundering provisions, age policies, anti-terrorist policies, anti-terrorist procedures, and responsible gambling policies requirements.

The third-party risk management team is trained on the:

- Extensive training on the back office tools in system, including the collusion algorithm.
- Training on the available reports, complementing the collusion tools.
- Player specific tools (blocking, monitoring tools).
- Disconnection protection mechanism.
- Chat block.
- How to detect collusion.
- Work procedures.
- Cash outs.

This anti-collusion team works directly with Customer Services and communication is ongoing between the teams to alert one another of any suspicious behavior from players. This includes rules that have been implemented and actions that may have been taken by the Fraud department.

Transaction monitoring system performance is reviewed annually, including testing of alerts for smurfing, layering, and crypto transactions. Independent AML audit or compliance review is performed at least annually to confirm control effectiveness.

12.2. Identity Verification Processes

The Company's platform provider integrates third party software resources, including age/identity verification providers outlined below. These are embedded within the system to ensure that Company is able to effectively identify its players. These verification providers are used in order to carry out the above due diligence procedures in line with Company policies.

- **GBGroup** – Provides international identity authentication services.
- **SHUFTI** - provides identity verification services, offering solutions for Know Your Customer (KYC), anti-money laundering (AML), and fraud prevention
- **Jumio** – identity verification, eKYC and AML solutions
- **FinCom** - Streamlined Data Search Solutions for AML/Sanctions Screening, Data Mapping,

Using multiple identity verification providers simultaneously allows Company to configure which identity verification services are applied to different players.

All supported identity verification services are integrated into the Automation Service Engine's condition language.

As a result the Company can determine when the identity verification should be carried out (immediately after signup, on the first deposit, and so on), for which players (by country, VIP level, and so on) and what the sanction should be if the verification fails (freeze the gaming account, block deposits and withdrawals, and so on)

The identity checks are triggered by fraud rules created on the configured Automation Rule Info.

13. Reporting of Unusual Transactions

When an employee knows or suspects, or the employee has reasonable grounds for knowing or suspecting that another person is engaged in money laundering or terrorist financing, it is incumbent on the employee to make a report to the Money Laundering Reporting Officer (MLRO). This includes any knowledge related to:

- Substantive criminal offences.
- Money laundering.
- Terrorist financing.
- Tipping off.
- Failing to report.

If a transaction or matter the employee is concerned about is not complete, the employee must not proceed with the issue unless advised to do so by the MLRO.

If an employee obtains knowledge or develops a suspicion after a transaction or matter has been completed, the employee must still report it to the MLRO as soon as possible/practical to do so.

Note: Failing to report a transaction or matter which is suspect, or where Company should have known or suspected to be related to money laundering or terrorist financing, Company or the employee responsible may face criminal prosecution.

13.1. Recognition of Unusual Transactions

Employees should be trained to identify unusual transactions based on customer profiles and specific indicators. This includes situations where:

- A potential customer hesitates to provide necessary identification.
- Unusual or suspicious identification is presented.
- A customer is reluctant to disclose the source of their funds.
- Multiple credit cards are used to deposit money in a short time frame.
- A large sum is deposited with minimal gameplay before withdrawal requests.
- Payment method locations do not match the customer's location.
- A customer requests to withdraw funds to a different account than that used for deposit.

- Any other actions suggest ulterior motives in using the company's services.

Failing to report a transaction or matter, which is suspect, or where the Company should have known or suspected to be related to money laundering or terrorist financing, the Company or the employee responsible may face criminal prosecution.

According to NORUT, the Company is observing both objective and subjective indicators to assess whether a customer's transaction is deemed unusual. All such transactions must be reported to the compliance officer in a format approved by management. Additionally, any supporting documentation, such as copies of identification, cash-out slips, and other relevant records, must also be submitted as supplements.

The Compliance Officer is tasked with maintaining an organized filing system for these records. If the casino fails to report internally identified transactions to the Financial Intelligence Unit (FIU), the rationale for this decision must be thoroughly documented and signed by the compliance officer and/or management. 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:

- Transactions which in connection with money laundering or terrorism financing are reported to the Police or to the Department of Justice;
- Transactions by or on behalf of a natural or legal person, a group or an entity, who is named on a list, adopted by virtue of the Sanctions National Ordinance (N.G. 2014 no. 55);
- Transactions in the amount of Cg. 5,000 or more, regardless of whether the transaction is made in cash, by check or other form of payment, or through electronic or other non-physical means. This includes but is not limited to:
 - A cashless transaction in the amount of Cg. 5,000 or more.
 - Accepting or releasing a deposit in the amount of Cg. 5,000 or more at the request of the customer;
 - Sale to a customer of chips in the amount of Cg. 5,000 or more. "Chips" include but is not limited to tokens and credits.
 - A cash out in the amount of Cg. 5,000 or more;
- Transactions where there is cause to presume that they can be related to money laundering or terrorist financing.

Examples of "red flags" include the following:

- A potential customer is reluctant to provide supporting evidence to enable identity verification.
- A potential customer presents unusual or suspicious identification documentation.
- A customer is reluctant to provide information in relation to the source of their wealth or funds.
- A customer uses multiple credit cards to deposit money within a short period of time (which may suggest the use of stolen cards).
- A customer deposits a large sum of money and makes a request to withdraw it having engaged in minimal or no gameplay.
- There is a mismatch between the customer's country of location and their payment method location.
- A customer uses one payment method to make a deposit and requests a withdrawal to be made to a different account.
- Any case where use of the Company services suggests ulterior motives.

The existence of a "red flag" leading to a suspicion that money laundering is taking place does not necessarily mean that money laundering is in fact taking place. It simply means that greater scrutiny is required and that a report should be made to the MLRO so that the MLRO can take any further steps that may be required to confirm or reject this suspicion.

13.2. Internal Reporting

As soon as knowledge is acquired or there is a suspicion of money laundering or terrorist financing the MLRO must be contacted. If the MLRO is unavailable, an alternative MLRO must be contacted. using an internal reporting form (see Appendix A). The CO will review the report within twenty-four (24) hours and determine if further investigation is necessary. If so, the investigation must be completed within five (5) business days, and the CO may request additional information from relevant departments.

Once the MLRO has been informed, the employee obligations are complete. It is advised that the employee does not pursue any form of investigation. The employee must follow the instructions provided by the MLRO.

13.3. External Reporting

Once the MLRO receives a report, the MLRO must consider it to determine whether it gives rise to grounds for knowledge or suspicion of money laundering.

The MLRO must assess the employee's report in conjunction with any information held about the customer's personal circumstances and in light of other transaction patterns and volumes through the customer's account.

The MLRO considers the matter in light of all the relevant information available within Company and decides whether or not to a disclosure needs to be made to the relevant authorities (known as a Unusual Transaction Report).

If the MLRO deems the activity unusual after their assessment, they are responsible for submitting an initial report to the Financial Intelligence Unit (FIU) regarding any suspicious monetary operations.

All reports and the reasoning behind any decisions made must be documented. The Compliance Officer must maintain organized records, including transaction details and any supporting documentation, for a minimum of five years from the end of the business relationship

13.4. Prohibition of Tipping Off

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 disciplinary action.

The employee must NEVER inform a customer or any third party that a report has been filed with the MLRO, that the MLRO has made a report to the authorities, or that an investigation is in contemplation or is underway. The employee must not tell a customer that a transaction is being delayed whilst consent to proceed is being sought from the authorities. This could constitute the offence of "tipping off".

13.5. Record Keeping

All documents, data and information collected to identify the client and to verify identity are retained for at least 5 years from the date on which the business relationship ends.

The records must be sufficient to enable a competent third party to assess the effectiveness of money laundering policies and procedures, including transaction records, due diligence information, suspicious transaction reports and AML training records.

Any suspicious transactions are recorded by the MLRO. Each report will consist of the date, the person reporting the activity and activity details. All suspicion reports are considered by the MLRO and where the MLRO decides not to make a disclosure to the authority, the reasons for the decision not to disclose are documented and retained. If the MLRO is uncertain, then the MLRO will automatically report this to the authority. The Company maintains a comprehensive Anti-Money Laundering, Counter-Terrorism Financing, and Counter-Proliferation Financing (AML/CTF/CPF) compliance program that is risk-based, proportionate to the nature and size of its operations, and designed to ensure full adherence to Curaçao's applicable legal and regulatory framework.

This program is structured around the following key principles:

Program Oversight

- The Compliance Officer has primary responsibility for the ongoing implementation and effectiveness of the AML/CTF/CPF program.
- Senior Management provides governance and oversight by reviewing the program on an annual basis and approving necessary enhancements.
- The program operates independently of the Company's commercial and gaming operations to ensure impartiality in compliance decision-making.

Independent Audit Function

- The Company shall engage an independent internal or external auditor to conduct a review of the AML/CTF/CPF program at least once per year.
- The audit will assess the adequacy, effectiveness, and consistent application of the Company's AML controls, including:
 - Customer due diligence and enhanced due diligence procedures;
 - Transaction monitoring and unusual transaction reporting processes;
 - Employee training and awareness;
 - Record-keeping practices.
- The auditor's findings will be reported to the Board of Directors, and corrective actions shall be documented and implemented without undue delay.

Blocking and Restricting Accounts

- The Company shall block or restrict customer accounts immediately where there are reasonable grounds to suspect that the account is being used for ML, TF, or PF purposes, or where documentary evidence required under CDD cannot be obtained within the regulatory timeframe.
- Any such action shall be promptly reported to the Compliance Officer and, where appropriate, an Unusual Transaction Report will be filed with the Financial Intelligence Unit (FIU) Curaçao.

Regulator and FIU Access

- The Company ensures that all policies, procedures, records, and supporting documentation relevant to AML/CTF/CPF compliance are made available to the Curaçao Gaming Authority (CGA), the FIU, or other competent authorities upon request and without delay.
- This includes customer identification data, risk assessments, transaction records, training registers, and audit reports, as relevant

Continuous Improvement

- Findings from independent audits, regulatory inspections, internal monitoring, and industry developments will be incorporated into periodic updates of the AML/CTF/CPF program.

- The Company is committed to adopting enhanced measures whenever new risks, products, or technologies emerge that may impact the effectiveness of its controls.

14. Consequences of Non-Compliance

The Company is committed to following all Curaçao AML, CTF, CPF, and sanctions laws, in line with FATF standards. Compliance with this Policy is mandatory for all employees, officers, agents, and third-party providers.

- Failure to comply may result in:
- Legal and regulatory action – fines, license suspension or revocation, and possible criminal prosecution.
- Reputational damage – loss of customer trust, negative publicity, and strained financial relationships.
- Operational impact – frozen funds, restricted access to financial systems, and increased regulatory scrutiny.

Employees who breach this Policy may face disciplinary measures, up to and including dismissal, and may be reported to law enforcement. Non-compliant third parties may have their contracts terminated.

All staff must complete training, follow procedures, and report unusual activity or policy breaches to the Compliance Officer. Whistleblowers are protected.

The Compliance Officer and senior management will investigate violations, decide on disciplinary or corrective measures, and report serious breaches to authorities. All cases are documented and used to strengthen the compliance program.

15. Related Policies and Procedures

The Company AML/CTF policies and procedures include customer due diligence, MLRO reporting, employee training and screening as well as internal controls to ensure adherence to the implemented policies and procedures.

To maintain vigilance against AML or CFT, Company has implemented the following policies and procedures:

- Know-Your-Customer (KYC) / Source-of-Funds (SOF)
- Reports any knowledge or suspicion that the company is being used for money laundering or terrorist financing purposes to the Money Laundering Reporting Officer (MLRO).
- Conducts ongoing relationship monitoring with existing customers and of transactions.
- Customers are required to notify Company of any changes to the initial information provided for the due diligence at the beginning of the business relationship.

16. Appendix A.

Company AML Unusual Activity Report

Reporting to Money Laundering Officer

Re: Suspicion of money laundering activity Reported to:

From:

Date:

Position:

DETAILS OF SUSPECTED OFFENCE

1. Name of person/business suspected:

2. Address/contact details of person/company suspected (if in possession of):

3. Full details of reasons for suspicion including: for example: what/where/how/value and any other details.

4. Have you discussed your suspicions with anyone else?

5. If yes- to whom and when?

Note: This form is subject to changes but can be used as a template to build forms more suited to different business opportunities.

Reporting to Regulatory Authorities as per license conditions