

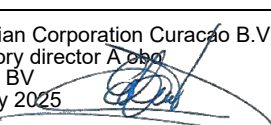
Swivel B.V.

AML, CFT & CFP POLICY

Document Information:

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

Version Control:

Date	Version	Summary Changes	Approved by Management
August 17, 2023	1.0	Policy implementation	
April 10, 2025	2.0	Policy update in line with CGA AML Regulations	Guardian Corporation Curacao B.V. Statutory director A. de Boer Swivel BV 30 May 2025 

For questions regarding this Policy please contact the designated Compliance Officer.

Table of Contents

POLICY STATEMENT	3
PURPOSE OF THE POLICY	3
DEFINITIONS	4
POLICY IMPLEMENTATION	7
<i>i. RESPONSIBILITY OF THE SENIOR MANAGEMENT</i>	<i>7</i>
<i>ii. COMPLIANCE OFFICER</i>	<i>7</i>
<i>iii. EMPLOYEES</i>	<i>7</i>
BUSINESS RISK ASSESSMENT	8
CUSTOMER RISK ASSESSMENT	8
CUSTOMER ACCEPTANCE POLICY	9
<i>iv. PROHIBITED CATEGORIES OF CUSTOMERS</i>	<i>9</i>
<i>v. CUSTOMER DUE DILIGENCE (CDD) MEASURES.....</i>	<i>9</i>
<i>vi. POLITICALLY EXPOSED PERSONS (PEPS)</i>	<i>10</i>
<i>vii. SANCTIONS SCREENING</i>	<i>10</i>
CUSTOMER DUE DILIGENCE (CDD).....	11
IDENTIFICATION AND VERIFICATION OF THE PLAYER	11
IDENTIFICATION AND VERIFICATION OF THE BENEFICIAL OWNER.....	12
TIMELINE FOR COMPLIANCE AND NON-COMPLIANT DOCUMENTS	12
ENHANCED DUE DILIGENCE (EDD).....	13
TARGETED FINANCIAL SANCTIONS	14
MONITORING.....	15
ONGOING CUSTOMER PROFILE MONITORING	15
ONGOING TRANSACTION MONITORING	15
REPORTING UNUSUAL ACTIVITIES AND TRANSACTIONS	16
A. INDICATORS OF UNUSUAL TRANSACTIONS.....	16
B. PROHIBITION OF DISCLOSURE	16
C. PROTECTION FOR REPORTING EMPLOYEES	16
RECORD-KEEPING.....	17
AML COMPLIANCE PROGRAM.....	18
STAFF RELIABILITY AND PROBITY	18
PROFESSIONAL SUPPORT AND TRAINING.....	18
COMPLIANCE AND CONSEQUENCES OF NON-COMPLIANCE	19

POLICY STATEMENT

The Policy on Prevention of Money Laundering, Terrorist Financing, and Proliferation Financing (hereinafter referred to as the "Policy") outlines the unified standards and procedures for anti-money laundering (AML) and combating the financing of terrorism (CFT) that must be followed by Swivel B.V., a Curacao-based operator of offshore games of chance (hereinafter referred to as the "Company").

It is the Company's responsibility to communicate the expected standards of AML requirements to its authorized operators and to provide them with a copy of this Policy for implementation. The Company may obtain quarterly certifications from its Authorized Operators to confirm their compliance with this Policy and applicable AML requirements.

This Policy offers general guidance on AML requirements that align with industry norms and standards relevant to the gaming sector. However, every entity to which this Policy applies must remain aware of and comply with applicable local AML regulations as they may change over time.

Compliance with this Policy is mandatory and crucial for ensuring that the Company fully adheres to the applicable AML and CFT laws and regulations of the respective countries and jurisdictions.

The Company is committed to conducting an annual review and critical reassessment of this Policy in light of its evolving business strategies, goals, and objectives.

PURPOSE OF THE POLICY

The purpose of this Policy is to establish a clear and structured framework that enables the Company to detect, prevent, and report any activities relating to money laundering, terrorist financing, and proliferation financing. This Policy articulates the minimum standards, roles, and responsibilities required to ensure compliance with all relevant legal and regulatory obligations under the jurisdiction of Curaçao.

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:

- National Ordinance of the 20th of December 2024 Containing Rules concerning Games of Chance (National Ordinance on Games of Chance) (PB 2024, no. 157);
- 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 Decree for general measures, of the 10 July 2015, for the implementation of article 2 of the Sanctions National Decree containing implementation of the United Nations' Security Council resolutions concerning Libya (Sanctions Ordinance Libya) (N.G. 2015 no. 28);
- National Decree for general measures, of the 10 July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of Resolutions 1695 (2006), 1718 (2006), 2087 (2013) and 2094 (2013) of the United Nations Security Council (Sanctions Decree People's Democratic Republic of Korea 2015) (N.G. 2015 no. 30);
- National decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of United Nations' Security Council

Resolutions concerning Al-Qaeda c.s., the Taliban of Afghanistan c.s., ISIL c.s. ANF c.s. and persons and organizations to be designated locally (N.G. 2015, no. 29);

- 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.

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. 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.

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.

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.

i. RESPONSIBILITY OF THE SENIOR MANAGEMENT

The Senior Management is responsible for:

- Set and approve the principles of the AML/CFT Policy.
- Appoint and communicate with the Compliance Officer.
- Define the roles and responsibilities of the Compliance Officers.
- Ensure systems and controls are effective for compliance.
- Provide Compliance Officers with timely access to necessary data (e.g., customer identity, transaction records).
- Ensure all employees know whom to report unusual transactions to.
- Provide adequate resources (staff and technology) for Compliance Officers.
- Assess and approve the annual report, addressing any identified weaknesses or deficiencies.

ii. COMPLIANCE OFFICER

The Company has appointed senior compliance officer will be designated, separate from our gaming operations, responsible for overseeing the AML program and ensuring compliance with regulations. Our AML/CFT 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.

The Compliance Officer has working knowledge of the Company's business environment, risks inherent to the Company's business model and AML&TF provisions as stipulated in the Regulations as amended.

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 casino'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 casino's efforts against money laundering and financing of terrorism and financing of proliferation.

iii. EMPLOYEES

-

BUSINESS RISK ASSESSMENT

The Company recognizes the requirement for all casinos to conduct a comprehensive Business Risk Assessment (BRA) to identify the money laundering (ML) and terrorist financing (TF) risks they may be exposed to. This assessment ensures that the policies, controls, and procedures in place are adequate to prevent and mitigate these risks. It specifically addresses how the Company's products and services could be misused for money laundering, financing terrorism, and financing proliferation, as well as the extent of those risks.

In conducting the BRA, the Company takes into account all relevant factors that may impact the risks of money laundering, financing of terrorism, and financing of proliferation. Special consideration is given to the types of customers, the products and services offered, the delivery channels, and geographical risk factors. The effectiveness of these measures is continuously monitored, and improvements are made as necessary.

The Company revises its business risk assessment whenever there are changes in the operational environment or business activities, such as the introduction of new payment methods, entry into new markets, the launch of new games, or changes in regulations. In the absence of significant changes, the business risk assessment is reviewed at least annually to evaluate whether updates are necessary.

This risk assessment is documented and must be approved by the Board of Directors. It should also be made available to the Gaming Control Board (GCB) upon request. The documentation includes the following aspects:

- The methodology adopted for the assessment
- The rationale for categorizing risk factors as low, medium, or high
- The outcomes of the BRA
- Any information sources utilized in the assessment

To operate on a risk-based approach, the Company commits to staying informed about the latest developments regarding money laundering and terrorist financing, ensuring that its policies and procedures remain effective and aligned with regulatory expectations.

CUSTOMER RISK ASSESSMENT

The Customer Risk Assessment procedure is a crucial component of the internal Anti-Money Laundering (AML) program at the casino, designed to evaluate the specific risks associated with providing services or products to customers. The assessment begins when a new customer applies for an account, at which point their risk profile is formulated based on the information collected. The initial Customer Risk Rating assigned helps determine the frequency and intensity of ongoing reviews; higher-risk customers will be subject to more frequent and rigorous monitoring.

The assessment process considers several key factors:

- o **Customer Risk:** This involves evaluating the customer's background, occupation, and transaction patterns. Higher-risk categories include customers with multiple or irregular income sources, politically exposed persons (PEPs), high spenders, disproportionate spenders (whose spending habits do not align with their known income), and those using third parties to gamble in ways that may circumvent customer due diligence measures.
- o **Product/Service Risk:** This factor assesses the risks associated with the casino's offerings. Certain gaming products or services, especially those allowing customers to influence outcomes, pose higher risks. Payment methods are also evaluated, with specific high-risk factors including anonymous payment options (like pre-paid cards and virtual assets), unusual account usage, peer-to-peer gaming, and multiple accounts or wallets. Additionally, identity fraud and the use of unlicensed electronic wallets are considered significant risks.
- o **Geographic Risk:** The geographic location of the customer and the transaction is assessed, with higher risk assigned to customers from countries with weak AML regulations or high corruption levels. Relevant sources of information include the FATF lists of high-risk jurisdictions, the U.S. Department of State's International Narcotics Control Strategy Report, and other credible indices. The nationality, residence, and place of birth of the player are also taken into account.

- o **Delivery Channel Risk:** This involves evaluating the methods used to establish a business relationship or conduct transactions. Channels that favor anonymity and non-face-to-face interactions are considered higher risk, prompting the Company to implement reasonable measures to mitigate these risks.

After the assessment, customers are categorized as low, medium, or high risk. The level of due diligence and ongoing monitoring applied corresponds to their risk classification:

- For customers assessed as low risk, a Simplified Due Diligence process will be applied, provided they do not exhibit any risk-enhancing characteristics and their transactions remain below the threshold of Cg. 4,000.
- Medium and high-risk customers will require additional information and documentation in accordance with the Company's policies.
- Accounts classified as high risk or displaying potentially suspicious behavior will be reviewed by compliance personnel and reported to the Compliance Officer (CO) for further investigation.

This structured approach ensures that the casino effectively identifies and mitigates the risks associated with its customers, aligning with regulatory expectations and promoting a robust AML compliance program.

CUSTOMER ACCEPTANCE POLICY

Company Name's Customer Acceptance Policy (CAP) is designed to ensure compliance with legal requirements while aligning with the Company's risk appetite and Business Risk Assessment (BRA). The CAP outlines the criteria for accepting customers, identifies higher-risk individuals, and delineates the necessary Customer Due Diligence (CDD) measures to mitigate risks associated with money laundering (ML), terrorist financing (TF), and proliferation financing (PF).

iv. PROHIBITED CATEGORIES OF CUSTOMERS

The Company will not accept customers who fall into the following categories:

- Individuals under the age of 18.
- Individuals listed on sanctions imposed by the UN, EU, or OFAC.
- Individuals with reasonable grounds to suspect involvement in ML, TF, PF, or any other criminal activity.
- Self-excluded customers who are barred from accessing our platforms or included in national self-exclusion registers as required by licensing conditions.
- Individuals who provide documents or information that the Company suspects to be fraudulent or falsified.

v. CUSTOMER DUE DILIGENCE (CDD) MEASURES

The level of CDD measures will be proportional to the risk classification:

- **Low and Medium Risk:** Simplified Due Diligence procedures will be applied, provided that the customer does not display any risk-enhancing characteristics and transactions remain below the threshold of Cg. 4,000.

- **High Risk:** Enhanced Due Diligence measures will be implemented, which include collecting additional information and documentation. For high-risk customers, ongoing monitoring will be more rigorous, including transaction reviews and alerts for unusual activity.

vi. POLITICALLY EXPOSED PERSONS (PEPS)

The Company implements robust procedures for identifying and managing relationships with PEPs, defined as individuals entrusted with prominent public functions, as well as their close associates and family members.

- **Identification:** Comprehensive screening against reliable databases will be conducted during the onboarding process to determine PEP status.
- **Approval Process:** No business relationship shall be established or continued with a PEP without obtaining senior management approval.
- **Source of Wealth and Funds:** The Company will request a statement from the PEP regarding their source of wealth and verify this information through independent and reliable sources. Additional documentation may be requested if necessary.
- **Enhanced Monitoring:** The Company will conduct enhanced ongoing monitoring of PEPs, analyzing their spending patterns to ensure they align with declared legal sources of funds.

PEP status screening will occur regularly throughout the business relationship. If a customer not identified as a PEP at onboarding later becomes one, the Company will implement enhanced due diligence measures within 30 days. Failure to implement these measures will result in the termination of the relationship with that customer.

vii. 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.

CUSTOMER DUE DILIGENCE (CDD)

The Company is required to perform Customer Due Diligence (CDD) under specific circumstances to ensure compliance with Anti-Money Laundering (AML) regulations and to protect the integrity of its operations. The Company must undertake CDD measures when players engage in financial transactions that amount to Cg. 4,000 or more. This includes any deposits or withdrawals made by the player.

In addition to financial transactions, the Company must carry out CDD for any occasional transaction that equals or exceeds Cg. 4,000. Furthermore, if there is any suspicion of money laundering (ML) or terrorist financing (TF), the Company is obligated to conduct CDD. This also applies in situations where there are doubts about the accuracy or completeness of previously obtained identification information from the player.

Financial transactions are defined specifically as deposits and withdrawals; bonuses are excluded from this category. Conversely, wagered amounts and winnings are classified as gambling transactions and do not fall under the definition of financial transactions. To effectively monitor and determine when a player reaches the Cg. 4,000 threshold for CDD purposes, the Company will evaluate not only individual transactions but also any series, combination, or pattern of transactions that exceed this amount. This evaluation will be conducted daily and will include all deposits, withdrawals, and peer-to-peer transfers made by the player.

Additionally, the Company maintains a strict policy against anonymous accounts or accounts held under fictitious names. The Company is committed to identifying each player by collecting their name and other relevant information, which is essential for determining the purpose and nature of the business relationship.

The main responsible department for the Due Diligence process is Factoring and Monitoring (Anti-fraud) Department. In order to perform the due diligence controls, employees use automatic controls, manual reviews and electronic registers.

IDENTIFICATION AND VERIFICATION OF THE PLAYER

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

- i. Full name;
- ii. Date of birth;
- iii. Permanent residential address;
- iv. Place of birth;
- v. Nationality; and
- vi. Identity number.

To complete the required customer identification and verification process, the Company asks its customers to upload a copy of valid identification documents (passport, identity card, driver's license, or an equivalent document). This request is sent to the customer's registered email address. If the documents are in a different language, the Company will take necessary steps to ensure that the documents adequately prove the customer's identity, such as obtaining a translation of the relevant parts. This may involve asking the customer to submit documents with a certified true translation.

Only documents issued by government agencies that include a photograph are deemed reliable for verifying the customer's identity. Government-issued documents that lack a photograph can be used to confirm the customer's current address, provided the address is included in the document. The Company accepts as proof of permanent residential address copies of utility bills (e.g., electricity, water, gas, telephone landline) or bank statements, as long as they are not older than six months at the time they are received.

IDENTIFICATION AND VERIFICATION OF THE BENEFICIAL OWNER

The Company is legally obligated to identify and verify the beneficial owner by confirming that customers are registering accounts to play and transact solely on their own behalf. Furthermore, players must declare that they are not acting on behalf of any third parties. The Company will not solely rely on this declaration. We are committed to actively monitoring player activity to detect any instances where a player may be using the account to play on behalf of others. This ongoing vigilance is essential to maintaining the integrity of our operations and ensuring compliance with AML-TF regulations.

To effectively manage this responsibility, the Company has implemented the following safeguards designed to prevent access to our services by individuals deemed suspicious:

- **Payment Method Verification:** Ensuring that the payment method used for deposits is in the name of the player, insofar as possible.
- **Denial of Service:** Preventing transactions for players attempting to use payment methods not in their own name.
- **Withdrawal Identity Verification:** Confirming the identity of players before processing withdrawals.

1. Understanding the Purpose and Intended Nature of the Business Relationship

While the primary purpose of a gaming account is clear, as part of our CDD measures, the Company must still collect relevant information to develop the customer profile. This involves understanding how a customer generated their net worth. The Company must assess whether this source justifies the projected and actual level of account activity. The extent of information collected must align with the risk rating identified during the Customer Risk Assessment (CRA).

For low- and medium-risk customers, the following measures are deemed sufficient:

- Information from open sources, including social media, can be a supplementary source for understanding a customer's profile.
- Obtaining a declaration from the customer detailing their nature of employment or business, along with their usual annual salary.

For high-risk customers, the following measures must be taken:

- Information provided by the customer must be substantiated by independent and reliable documentation. This could include tax returns, salary slips, or bank statements.
- The Company should collect comprehensive details about the sources of wealth to understand the financial background of high-risk customers.

To analyze and verify this information, the Company may take into account the average national income, average disposable income, and other relevant metrics to gauge expected wagering power based on jurisdiction. This is done in consultation with the risk-based approach, whereby the extent of the mitigation will be based on the identified risks. The customer risk profile developed through this process serves as the foundation for the ongoing monitoring of player activity.

TIMELINE FOR COMPLIANCE AND NON-COMPLIANT DOCUMENTS

If the customer cannot provide compliant documents within 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 threshold, 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.

ENHANCED DUE DILIGENCE (EDD)

The Company shall implement Enhanced Due Diligence (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.
- Politically Exposed Persons (PEPs): Individuals who hold prominent public positions or are closely connected to such individuals, which may elevate the risk of corruption.
- Anonymity-favoring 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.

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. 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.

TARGETED FINANCIAL 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 United Nations (UN) and European Union (EU) as being involved in terrorism or proliferation activities. Mechanisms are established to ensure compliance with the Company's legal obligations. This includes, but is not limited to, the following:

- The Company shall comply with relevant sanctions decrees and regulations and monitor any and all amendments thereof and implement these without undue delay.
- The Company shall perform ongoing sanctions screening on customers and also conduct 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 changes to personal details or payment methods.

In the event that a true match is discovered and confirmed, the Company must immediately proceed with freezing the funds of the particular customer(s), in accordance with the Sanctions Ordinance, and must 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, or otherwise, in light of tipping-off considerations, follow instructions from the supervisory authority.

MONITORING

ONGOING CUSTOMER PROFILE MONITORING

During the periodic review of a customer, Company Name 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.

ONGOING TRANSACTION MONITORING

Company Name 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).

REPORTING UNUSUAL ACTIVITIES AND TRANSACTIONS

The Company is committed to identifying and reporting any unusual activities and transactions, including attempted transactions, to ensure compliance with Anti-Money Laundering (AML) regulations. This section outlines the procedures and responsibilities for recognizing, reporting, and investigating unusual transactions.

Employees must report any unusual activity to the Compliance Officer immediately, but no later than 24 hours after the transaction has been executed. This includes any transactions that raise suspicion or deviate from normal behavior.

Employees must submit an Internal Unusual Activity Report (IUAR) to the Compliance Officer. The format of the internal report on unusual activities and transactions is provided in Appendix C.

If a more in-depth investigation is required, the Compliance Officer may request additional information from relevant departments. This investigation must be completed within ten (10) business days.

The Compliance Officer will assess the information available to determine if it is sufficient to warrant filing an Unusual Transaction Report (UTR) with the Financial Intelligence Unit (FIU).

If the Compliance Officer concludes that the activity is unusual, a report shall be submitted to the FIU regarding any unusual monetary operations or transactions within 48 hours.

a. INDICATORS OF UNUSUAL TRANSACTIONS

The Company observes both objective and subjective indicators to assess whether a customer's transaction is deemed unusual. The following transactions or intended transactions are considered unusual:

1. A transaction reported to law enforcement or judicial authorities in connection with money laundering or terrorism financing.
2. An intended transaction carried out by or for the benefit of any individual, legal entity, or group identified on a sanctions list.
3. A transaction amounting to NAf. 5,000.00 or more, regardless of the payment method, which includes:
 - A cashless transaction in the amount of NAf. 5,000.00 or more.
 - Accepting or releasing a deposit of NAf. 5,000.00 or more at the customer's request.
 - Sale of chips to a customer amounting to NAf. 5,000.00 or more.
 - A cash-out transaction of NAf. 5,000.00 or more.
4. Transactions that may reasonably be presumed to relate to money laundering or terrorist financing.

b. PROHIBITION OF DISCLOSURE

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

c. PROTECTION FOR REPORTING EMPLOYEES

The Company has implemented measures to safeguard employees and representatives who report suspicions of money laundering, terrorist financing, and/or financing of proliferation to the FIU. Employees reporting such suspicions are protected from threats or hostile actions by other employees, management, or customers, as well as from adverse or discriminatory employment actions.

RECORD-KEEPING

The Company retains all necessary records of transactions, both domestic and international, for a minimum of five (5) years to ensure compliance with information requests from regulatory authorities. These records must be detailed enough to allow for the reconstruction of individual transactions, including the amounts and types of currency involved, if applicable, to provide evidence for potential criminal prosecutions.

All records gathered through CDD measures, such as copies of official identification documents, account files, and business correspondence, will be stored for at least five (5) years after the business relationship has ended or after the date of an occasional transaction.

Records shall be stored in a manner that ensures their integrity, confidentiality, and accessibility. Access is restricted to authorized personnel only. Regular backups of electronic records shall be conducted and stored in a separate, secure location to prevent data loss.

After the retention period, records shall be disposed of securely to prevent unauthorized access or disclosure.

When properly ordered to do so by any enactment, rule of law or court order, the Company shall provide a document, customer due diligence information, or enhanced due diligence information and the Company will maintain a register of the documents and information provided and will keep a copy of the same.

AML COMPLIANCE PROGRAM

STAFF RELIABILITY AND PROBITY

The Company has established HR policies and procedures for effective initial candidate screening and ongoing employee management. All personnel undergo a personal identification process, and candidates must complete an ID profile that includes psychological tests during their first interview to assess potential risks. After the initial interview, successful candidates participate in a second interview with the HR Director, followed by discussions with the subject area manager and a member of the internal security department. A thorough background check is conducted, which includes contacting previous supervisors, verifying criminal records, and reviewing job references.

Once candidates successfully complete the screening process, they are required to undergo a mandatory three-week introductory training course divided into five stages, covering bookmaking basics, payment systems, software usage, customer complaint handling, and workplace training. After passing all exams, new employees begin their roles under close supervision. For executive positions, candidates must have a personal interview with the CEO or owner before a hiring decision is made.

PROFESSIONAL SUPPORT AND TRAINING

The Company is committed to supporting employees' professional development through various training opportunities, including on-site and remote training, technical seminars, and workshops. Employees receive training in relevant business areas, with management training focusing on effective management practices and business English courses available for all staff. Specialized professional upgrade courses are conducted internally for Trading and Operational Department staff, while the Marketing and Finance Departments participate in targeted training sessions relevant to their fields.

In addition, refresh training sessions are conducted periodically, at least annually, to ensure employees remain up-to-date with current practices. Specific events, such as the introduction of new systems or technologies—especially those that have a higher potential for misuse in money laundering—will trigger additional training sessions. Significant violations of this policy will also prompt targeted training to reinforce compliance expectations.

Additionally, the Compliance Officer conducts mandatory introductory Anti-Money Laundering and Terrorism Financing (AML&TF) training for all new employees, which covers their roles in compliance, identifying red flags for money laundering, and the procedures for reporting suspicious activities. This training is supplemented with updates on the latest tools and practices in AML&TF investigations. The Compliance Officer maintains a register of all trained employees involved in monitoring transactions and compliance management.

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 the AML/CTF 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.