

ANTI-MONEY LAUNDERING, COUNTER-
TERRORISM FINANCING, AND COUNTER-
PROLIFERATION FINANCING
(AML, CTF AND CPF) POLICY

CONFIDENTIAL

Table of Contents

1	PREFACE	4
1.1	COMPLIANCE STATEMENT.....	4
1.2	APPLICABLE LEGISLATION.....	4
1.3	DOCUMENT MAINTENANCE AND REVIEW	5
1.4	DEFINITION OF MONEY LAUNDERING	5
1.5	DEFINITION OF FINANCING OF TERRORISM.....	6
1.6	DEFINITION OF FINANCING OF PROLIFERATION OF WEAPONS	7
1.7	TARGETED FINANCIAL SANCTIONS	7
2	THE RISK-BASED APPROACH	8
2.1	EXPLANATION OF THE RISK-BASED APPROACH	8
2.2	BUSINESS AND CUSTOMER RISK ASSESSMENTS.....	8
2.2.1	<i>Business Risk Assessment</i>	<i>8</i>
2.2.2	<i>Customer Risk Assessment.....</i>	<i>9</i>
3	CUSTOMER DUE DILIGENCE (CDD).....	10
3.1	CUSTOMER ACCEPTANCE.....	10
3.1.1	<i>Risk Indicators.....</i>	<i>10</i>
3.1.2	<i>Prohibited Accounts</i>	<i>12</i>
3.2	CDD MEASURES	12
3.3	ENHANCED DUE DILIGENCE	14
3.4	SIMPLIFIED DUE DILIGENCE.....	15
3.5	POLITICALLY EXPOSED PERSONS (PEPs)	15
3.5.1	<i>Foreign PEPs</i>	<i>16</i>
3.5.2	<i>Domestic PEPs.....</i>	<i>17</i>
3.6	ONGOING MONITORING	17
3.6.1	<i>Ongoing Customer Profile Monitoring.....</i>	<i>17</i>
3.6.2	<i>Ongoing Transaction Monitoring</i>	<i>18</i>
4	REPORTING UNUSUAL TRANSACTIONS.....	19
4.1	REPORTING OBLIGATIONS	19
4.2	RECOGNITION OF UNUSUAL TRANSACTIONS.....	19
4.3	PROHIBITION OF DISCLOSURE	20
4.4	RECORD KEEPING	21
5	ANTI-MONEY LAUNDERING COMPLIANCE PROGRAM	22
5.1	APPOINTMENT OF A MONEY LAUNDERING COMPLIANCE OFFICER	22
5.1.1	<i>Duties of the Compliance Officer.....</i>	<i>22</i>
5.2	EMPLOYEE SCREENING AND TRAINING PROGRAMS.....	22
5.2.1	<i>Employee Due Diligence</i>	<i>22</i>
5.2.2	<i>Training.....</i>	<i>23</i>
5.3	INDEPENDENT AUDIT FUNCTION	24
6	APPENDIX I: COUNTRY RISK LIST	25
7	APPENDIX II: INTERNAL UNUSUAL ACTIVITY REPORT	28

Document Information

Subject	Anti-Money Laundering, Counter-Terrorism Financing, and Counter-Proliferation Financing (AML, CTF and CPF) Policy
Impact	All Departments
Responsibility	Money Laundering Reporting Officer
Approval	Directors
Review	Annually or as Needed
Classification	Company Confidential

Version History

Date	Ver.	Author	Summary Changes	Submitted to MGA
04.12.2024	1.0	Palau Holdings N.V.	Document created as part of AML Program review	

1 Preface

1.1 Compliance Statement

Palau Holdings N.V. (the Company), being established in and governed by the laws of Curaçao, is committed to implementing robust policies to prevent money laundering (ML), terrorism financing (TF), and proliferation financing (PF). In light thereof, the Company has developed a comprehensive Anti-Money Laundering, Counter Terrorism Financing and Counter Proliferation Financing (AML, CTF AND CPF) policy. Adherence to this Policy is obligatory and vital for guaranteeing that the Company remains in full compliance with relevant laws and regulations pertaining to AML, CTF AND CPF. As a responsible gaming enterprise operating in Curaçao, we acknowledge the paramount importance of upholding the integrity of our financial systems and preventing the exploitation of our operations for unlawful activities. Our commitment to compliance transcends mere legal requirements; it is a core component of our corporate responsibility and ethical principles.

1.2 Applicable Legislation

The local authorities in charge of the supervision of AML/CFT/CFP matters for the gaming sector are the Curaçao Gaming Control Board (GCB) and the Curaçao Financial Intelligence Unit (FIU). 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:

- The Code of Criminal Law (Penal Code) (N.G. 2011, no. 48);
- The National Ordinance on Identification of Customers when Rendering Services (NOIS) (N.G. 2017, no. 92), last update June 2024;
- The National Ordinance on the Reporting of Unusual Transactions (NORUT) (N.G. 2017, no. 99), last update June 2024;
- 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);
- National Decree penalties and fines reporting unusual transactions (N.G. 2021, no. 69) as amended by PB 2023, no. 6.;
- National Decree supervisor identification when rendering services gaming sector (L.B. 28.01.2019, no. 19/0282)
- National Decree supervisor unusual transactions gaming sector (L.B. 28.01.2019, no. 19/0283)
- 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 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);
- 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 prohibition of import, export, and transit of Venezuelan Gold (N.G. 2019, no. 82).
- National Ordinance on the Obligation to report Cross-border Money Transportation (N.G. 2002, no.74) as amended by (N.G. 2014, no. 90).
- GCB's Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction, last update May 2024.

The Company's operations are guided by collaboration with international regulatory bodies, including the Financial Action Taskforce (FATF) and the Caribbean Financial Action Task Force (CFATF), strengthening our compliance with global standards.

1.3 Document Maintenance and Review

This AML, CTF AND CPF policy is designed to meet the legal requirements as outlined by the Gaming Control Board of Curaçao and to foster a culture of compliance within our organization.

Regular reviews and updates will be conducted to adapt to evolving regulations and business needs. The maintenance and review of this document will take place annually.

1.4 Definition of Money Laundering

Money laundering (ML) is the process of concealing the true origins of illegally obtained funds, making them appear to originate from legitimate sources. Money laundering encompasses a broad range of activities, including attempts to turn criminally obtained money into 'clean' money, transferring the benefits of crimes like theft or fraud, and facilitating the laundering of criminal or terrorist property. This process typically occurs in three stages:

- *Placement*, where illegal proceeds are introduced into the financial system through financial institutions, casinos, or cash-intensive businesses, often by converting cash into monetary instruments or gaming chips. In the gambling industry, this is occasionally achieved by purchasing chips with cash and subsequently redeeming their value without engaging in actual gameplay or with minimal play. It can also involve funding casino accounts using credit and debit cards, prepaid cards, checks, and cryptocurrency, followed by requests for payouts or inserting funds into gaming machines and immediately claiming those funds as credits.
- *Layering*, which involves transferring or moving these funds across various accounts or financial institutions to obscure their criminal origins. In the gambling industry, this may include transactions such as transferring funds between accounts, occasionally involving other casinos or jurisdictions, currency exchanges, structuring and refining transactions, as well as maintaining gambling accounts to store money and conceal it from regulatory authorities; and
- *Integration*, where the laundered funds are reintroduced into the economy, enabling their use in legitimate transactions such as purchasing luxury assets or investing in businesses.

As it is strict Company policy not to accept cash as means of payment, the Company's AML Policy is conducive the curtailment of AML risk.

1.5 Definition of Financing of Terrorism

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. Unlike money laundering, which always involves proceeds from illegal activities, terrorist financing may not necessarily derive from illicit sources; instead, it often utilizes legitimate funds from charitable donations, business profits, or foreign government sponsorships. While both terrorism financing and money laundering may employ similar methods – such as cash smuggling, structuring, wire transfers, and the use of debit and credit cards – the primary concern of TF is to obscure the intended use or end recipient of the funds rather than their origin. Additionally, funding for terrorist activities does not always require large sums of money, as it can accumulate over time through simple transactions.

The gaming sector, especially online platforms, can be particularly vulnerable to exploitation by terrorist groups looking to launder money or transfer funds discreetly, due to its inherent anonymity and high transaction volumes. Ultimately, the goal of terrorism financing is to facilitate the planning, preparation, and execution of acts that threaten both national and international security.

1.6 Definition of Financing of Proliferation of Weapons

Financing of proliferation (FP) 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.

1.7 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 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 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.

2 The Risk-Based Approach

2.1 Explanation of the Risk-Based Approach

The Company adopts a risk-based approach in our AML compliance program, as recommended by FATF guidelines. This approach is essential for identifying and mitigating ML/TF risks specific to the online gaming industry. 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.

2.2 Business and Customer Risk Assessments

2.2.1 Business Risk Assessment

The Business Risk Assessment (BRA) framework is an essential element of the Company's AML/CFT/CPF compliance program. It offers a systematic risk-based approach to identifying, assessing, and mitigating the risks associated with money laundering, terrorist financing, and proliferation financing within the Company's operations.

The Company conducts comprehensive BRAs and evaluates potential risk factors related to customers, products, services, geographic locations, and delivery channels. Each identified risk factor is assessed based on its likelihood and potential impact, utilizing both quantitative and qualitative data. Appropriate controls and measures are then implemented to address the identified risks, tailored to the specific level and nature of the threat. All findings, evaluations, and mitigation strategies are documented and reported to senior management and relevant regulatory authorities.

BRAs are conducted regularly to ensure that the Company's risk profile stays current and accurate, with a comprehensive assessment performed annually. Additional assessments may be prompted by significant events, such as the launch of new products, changes in regulations, or substantial shifts in the business landscape.

2.2.2 Customer Risk Assessment

The Customer Risk Assessment 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.

3 Customer Due Diligence (CDD)

3.1 Customer Acceptance

3.1.1 Risk Indicators

The determination of the customer risk rating is first assigned when a new customer applies for an account. This rating helps decide how often and in what way the customer will be reviewed in the future: higher risk means more frequent reviews.

The customer risk rating plays a crucial role in the entire CDD process. It helps determine how thorough the verification process will be and what extra documents or information are needed to manage the identified risks. Additionally, it guides the monitoring of the customer, as the risk level dictates how often monitoring and reviews occur.

The risk assessment process takes into consideration the following factors:

3.1.1.1 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).

3.1.1.2 Product/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.

3.1.1.3 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 considered as these might be indicative of a heightened geographical risk. The Company regards 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. Please see [Annex I](#).

3.1.1.4 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.

3.1.2 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:

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

3.2 CDD Measures

The Company has an obligation to undertake CDD measures when:

- players engage in financial transactions equal to or above Naf. 4,000.00;
- carrying out occasional transactions above the monetary equivalent of Naf. 4,000.00;
- there is a suspicion of money laundering or terrorist financing; or
- the casino 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.

The Company's CDD procedures require prospective customers to create a full profile at the 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.

To complete the required customer identification and verification process, the Company asks its customers to upload a copy of valid identification documents. This request is sent to the customer's registered email address. If needed, the customer may also receive a phone call to help with the verification process. 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. Documents issued by the government that lack a photograph can be used to confirm the customer's current address, provided the address is included in the document.

If a document submitted by a potential customer does not meet the verification standards, the compliance officer or 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. If the customer cannot provide compliant documents within 30 days from the moment the Naf. 4,000.00 threshold is reached, the Company shall terminate the relationship with the customer and report the transaction to the FIU.

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.

3.3 Enhanced Due Diligence

Enhanced Due Diligence (EDD) will be implemented for customers identified as higher risk, consistent with the risks identified. In particular, they should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual. Enhanced Due Diligence has to be conducted where the risks of money laundering or terrorist financing are higher. In any case, the following scenarios are subject to EDD:

- Residents of higher risk geographic areas;
- Politically Exposed Persons (PEP's);
- Products or transactions that might favor anonymity;
- New products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products.

The applied measures must be consistent with the risks identified. They should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious. Examples of EDD measures include but are not limited to:

- Obtaining additional information on the customer, like occupation, previous address and information available through public databases, internet, etc.;
- Obtaining additional information on the intended nature of the business relationship;
- Obtaining information on the source of funds or source of wealth of the player:
 - **Source of Funds** refers to the origin of the specific funds involved in a particular transaction. This includes identifying how and where the money was generated, such as through salary, business income, or sale of assets. For politically exposed persons (PEPs), it is crucial to verify that the funds used in transactions are legitimate and not derived from illicit activities.
 - **Source of Wealth**, on the other hand, pertains to the total accumulation of an individual's wealth over time. This includes understanding the broader context of

their financial background, such as investments, property ownership, and other significant assets.

- Obtaining information on the reasons for intended or performed transactions;
- Obtaining the approval of senior management to commence or continue the business relationship;
- Conducting enhanced monitoring of the business relationship;
- Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

3.4 Simplified Due Diligence

In low-risk scenarios, where the risks of ML/TF/PF are lower, simplified due diligence measures may be applicable, balancing the need for compliance with operational efficiency. Such measures include but are not limited to:

- *Not collecting specific information:* If the risk assessment undertaken indicates a low risk of money laundering or terrorist financing then it is only necessary for the casino to obtain the player's identity.
- Verifying the identity of the customer and the beneficial owner *after* the establishment of the business relationship;
- The extent of verification may also vary depending on the risk posed by the particular business relationship. In a low-risk situation, the Company can also use alternative reputable information sources, even where these do not contain photographic evidence of the player's identity (e.g. birth certificates, bank statements etc.);
- The extent of personal details verified can also vary. In low-risk situations, the Company has to verify the basic identification details, while the verification of any other personal details is upon the Company, as long as it has sufficient comfort that it knows who its customer is;
- Reducing the frequency of customer identification updates;
- Reducing the degree of ongoing monitoring and scrutinizing transactions, based on a reasonable monetary threshold.

Simplified CDD measures are not acceptable whenever there is suspicion of money laundering or terrorist financing, or where specific higher-risk scenarios apply, or when the customer reaches the threshold prescribed above of Naf. 4,000.00.

3.5 Politically Exposed Persons (PEPs)

A PEP is an individual who is entrusted with prominent public functions, other than middle ranking or more junior officials, including the following individuals:

- heads of state, heads of government, ministers and deputy or assistant ministers,
- members of parliament or of similar legislative bodies,

- members of the governing bodies of political parties,
- members of supreme courts, constitutional courts or other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances,
- members of courts of auditors or of the boards of central banks,
- ambassadors, chargés d'affaires and high-ranking officers in the armed forces,
- members of the administrative, management or supervisory bodies of state-owned enterprises
- directors, deputy directors and members of the board or equivalent function of an international organization.

The following individuals are also regarded as PEPs by virtue of their relationship or association with the individuals listed above:

- family members of the individuals listed above, including spouse, partner, children and their spouses or partners, and parents
- known close associates of the individuals listed above, including individuals with whom joint beneficial ownership of a legal entity or legal arrangement is held, with whom there are close business relations, or who is a sole beneficial owner of a legal entity or arrangement set up for the benefit of the PEP.

To identify if a client should be regarded as PEP the Company uses a variety of methods containing sufficient resources. The Company, on an ongoing basis, verifies whether its customers may be considered as PEPs by utilizing open sources and public databases. Should a player who had not been identified as a PEP at on-boarding stage result to have become one, the casino is required to implement the measures described below in 3.5.1 and 3.5.2 within 30 days or terminate the relationship.

The requirements for the CDD of PEPs, as listed below in 3.5.1 and 3.5.2, shall apply also to relatives and close associates of PEPs, as defined in this Policy.

3.5.1 Foreign PEPs

With respect to customers that have been confirmed as foreign PEPs, the Company shall:

- a. have appropriate risk-management systems to determine whether the customer or the beneficial owner is a politically exposed person;
- b. obtain senior management approval to service the PEP (for establishing the business relationship for new customers, continuing the business relationship for existing customers or for conducting the occasional transaction). Senior management are the persons who determine the day-to-day operations or those directly below the level of those determining the day-to-day operations. The approval can also be given from the manager of the Compliance department;

- c. take reasonable measures to establish the source of wealth and the source of funds. The investigation must then determine whether the player's spending pattern matches his legal source of funds. The casino requests a statement from the player about the source of funds and verifies them by consulting independent and reliable sources. Depending on the risk in specific cases, this can in the first place be public sources. When public sources cannot, or can insufficiently verify the information received, the casino can request the customer to provide documents. For PEPs, assessing the source of wealth helps ensure that their overall wealth is consistent with their known income and legitimate activities, thereby mitigating the risk of money laundering or terrorism financing.; and
- d. conduct enhanced ongoing monitoring of the business relationship.

3.5.2 Domestic PEPs

The Company shall take reasonable measures to determine whether a customer is a domestic PEP or a person who is or has been entrusted with a prominent function by an international organization. In cases of a higher risk business relationship with such persons, casinos are required to apply the measures referred to in items b, c and d section 3.5.1. In accordance with the risk-based approach that the Company employs, measures are tailored to the risk of the PEP, where the following are taken into consideration:

- the type of public function of the PEP;
- the country from which the PEP originates;
- the transactions that the PEP carries out.

3.6 Ongoing Monitoring

3.6.1 Ongoing Customer Profile Monitoring

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

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

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

3.6.2 Ongoing Transaction Monitoring

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

4 Reporting Unusual Transactions

4.1 Reporting Obligations

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

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

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

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

4.2 Recognition of Unusual Transactions

Staff will be trained to recognize unusual transactions based on customer profiles and specific indicators. Reporting procedures to the compliance officer will be established.

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:

- a. A transaction, which is reported to the police or judicial authorities in connection with money laundering or the financing of terrorism;
- b. An intended transaction carried out by or for the benefit of a natural person, legal person, group or entity which is on a list compiled by virtue of the Sanctions National Ordinance (N.G. 2014 no. 55);
- c. A transaction amounting to Naf. 5,000.00 or more, regardless of whether this transaction is carried out in cash, via a check or another payment instrument or electronically or in any other non-physical manner. This includes but is not limited to:
 1. A cashless transaction in the amount of Naf. 5,000.00 or more.
 2. Accepting or releasing a deposit in the amount of Naf. 5,000.00 or more at the request of the customer;
 3. Sale to a customer of chips in the amount of Naf. 5,000.00 or more. "Chips" include but is not limited to tokens and credits.
 4. A cash out in the amount of Naf. 5,000.00 or more;
- d. Transactions where there is cause to presume that they can be related to money laundering or terrorist financing.

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

4.3 Prohibition of Disclosure

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

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

4.4 Record Keeping

The casino 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. Electronic records shall be stored in secure, encrypted databases with access controls to prevent unauthorized access. Physical records shall be stored in locked, fireproof cabinets within secure areas of the office. 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. Electronic records must be permanently deleted using secure deletion software that ensures data cannot be recovered. Physical records must be shredded using cross-cut shredders or incinerated to ensure complete destruction.

5 Anti-Money Laundering Compliance Program

5.1 Appointment of a Money Laundering Compliance Officer

A senior compliance officer will be designated, separate from our gaming operations, responsible for overseeing the AML program and ensuring compliance with regulations. Our AML/CTF 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.

5.1.1 Duties of the Compliance Officer

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

- To design and implement the AML program;
- To verify adherence to local laws and regulations regarding the detection and deterrence of money laundering and terrorist financing;
- To review compliance with the 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.

5.2 Employee Screening and Training Programs

5.2.1 Employee Due Diligence

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

The employee due diligence process is informed by the Company's risk assessment and the specific roles within the organization.

Any employee whose position may enable them to facilitate money laundering or terrorism financing must undergo screening. This requirement applies to:

- Prospective employees prior to their hiring for such roles.
- Current employees before they are transferred or promoted to such positions.

To screen both current and potential employees, the Company should:

- Identify the individuals.
- Verify their identity.
- Confirm their employment history, such as through references.
- Determine their suitability for the position and assess whether they pose any risk to the Company.

The Company will consider the knowledge and qualifications required for the responsibilities and authorities associated with each role.

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

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

Regular updates and re-evaluations are essential for maintaining an effective compliance program against money laundering, terrorism financing, and proliferation financing. This process includes conducting periodic reviews of all employees, with a particular emphasis on those in high-risk roles, to ensure their risk profiles are accurate and current. Additionally, reviews triggered by significant changes in an employee's job responsibilities, promotions, or external alerts that may influence their risk status are also initiated.

5.2.2 Training

In delivering AML, CTF and CPF training to the designated categories of employees, the Company will consider the necessary knowledge and qualifications required for their duties, responsibilities, and authorizations. As part of the training framework, the Company will outline the AML, CTF and CPF requirements and provide comprehensive information on the measures and activities that staff are expected to undertake within their roles.

The Company will ensure that documentation of the training provided to staff is maintained, capturing the following information:

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

The Company will regularly update the training programs to reflect any changes in internal and external regulations, as well as developments in the availability of training programs in the market for external training. Furthermore, extraordinary training in AML, CTF and CPF matters will be provided in specific situations, including:

- The introduction of new internal and external regulations related to AML, CTF and CPF that apply to the Company's staff.
- The launch of new products or services that alter the AML, CTF and CPF risk exposure.
- Instances where an employee breaches internal or external AML, CTF and CPF regulations due to a lack of knowledge during the performance of their duties.

5.3 Independent Audit Function

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

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

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

6 Appendix I: Country Risk List

Please note that the following list of high-risk and low-risk countries is subject to continuous review. Any changes in geographical risk will be reflected promptly to ensure the list remains current and accurate at the time of drafting.

High-risk countries include:

1. Afghanistan
2. Algeria
3. Angola
4. Belarus
5. Bulgaria
6. Burkina Faso
7. Burma (Myanmar)
8. Cameroon
9. Central African Republic
10. China
11. Côte d'Ivoire
12. Croatia
13. Cuba
14. Democratic People's Republic of Korea.
15. Democratic Republic of the Congo
16. Ethiopia
17. Gibraltar
18. Haiti
19. Iran
20. Iraq
21. Kenya
22. Lebanon
23. Libya
24. Mali
25. Monaco
26. Mozambique
27. Namibia
28. Nicaragua
29. Nigeria
30. Panama
31. Philippines
32. Russia
33. Somalia

34. South Africa
35. South Sudan
36. Syria
37. Tanzania
38. Uganda
39. United Arab Emirates
40. Vanuatu
41. Venezuela
42. Vietnam
43. Yemen

Low-risk countries include:

1. Antigua and Barbuda
2. Aruba, Kingdom of the Netherlands
3. Belize
4. Bermuda
5. Cayman Islands
6. Denmark
7. Dominica
8. Finland
9. Grenada
10. Guyana
11. Montserrat
12. New Zealand
13. Norway
14. Saint Kitts and Nevis
15. Saint Lucia
16. Saint Vincent & the Grenadines
17. Singapore
18. Sint Maarten Kingdom of the Netherlands
19. Suriname
20. Sweden
21. Turks and Caicos Islands

Excluded markets include, but are not limited to:

1. Aruba
2. Australia
3. Austria
4. Belgium
5. Bonaire

6. Czech Republic
7. Curacao
8. France
9. Germany
10. Greece
11. Lithuania
12. Saba
13. Sint Eustatius
14. Spain
15. The Netherlands
16. United States of America

CONFIDENTIAL

7 Appendix II: Internal Unusual Activity Report

Internal Unusual Activity Report		
Date of report:		
Client full name:		
Client ID:		
Risk rating:		
Account status (Active/Suspended/Blocked):		
Account balance:		
Date of account registration:		
Client details: E-mail:		
Client details: Phone number:		
Client details: Brand registration:		
Date of birth:		
Nationality/Country of registration:		
Address:		
Due diligence documents held:		
Reason for reporting: explain what activity / transaction gave rise to the report. If necessary, please use the additional information section:		
Date of suspected criminal activity/transaction:		
Provide details (e.g. dates and amounts) of any known intended or pending transactions:		
Name (reporting employee):	Signature:	Date:

PALAU HOLDINGS N.V. AML, CTF & CPF POLICY

Upon completion, please forward the form to the department responsible as soon as possible.		
Action taken by the responsible department		
Confirmation of receipt of the MLRO: I confirm that I have received this form from the person(s) named above.	Signature:	Date: