

Pelican Entertainment B.V.

AML/CTF/CPF Policy

Version 1	By the Board of Directors
Approved on December 5, 2024	

(SMES)
Solutions for Management
and Employment Support N.V.

Contents:

1. Purpose and Scope of Policy
2. Online Gaming Environment & Specifics
3. Assessment of Risks: Money laundering, Terrorism Financing & Proliferation Financing
 - 3.1. Anti-Money Laundering
 - 3.2. Counter-Terrorism Financing
 - 3.3. Counter-Proliferation Financing
 - 3.4. Risk-Based Approach
 - 3.5. Key Risk Areas Specific to Gambling Sector
 - 3.5.1. Distribution Channel Risks
 - 3.5.2. Customer Risk
 - 3.5.3. Mitigation Strategies for Customer Risk
 - 3.5.4. Product, Service & Transaction Risks
 - 3.5.5. Geographic Risks
 - 3.5.6 Company's Strategies to Mitigate Geographic Risks
4. Senior Management Duties & Responsibilities
5. Customer Due Diligence
 - 5.1. Player Identification & Verification
 - 5.2. Understanding the Purpose and Nature of Business Relationships
 - 5.3. Continuous Monitoring of Identity and Transactions
 - 5.4. Enhanced Due Diligence (EDD)
 - 5.5. Simplified Due Diligence (SDD)
 - 5.6. protocol for Politically Exposed Persons (PEPs)
 - 5.7. Reliance on Third-Party Providers and Technological Tools
 - 5.8. Termination of Business Relationships
6. Sanctions
7. Compliance Officer
 - 7.1. Appointment
 - 7.2. Key Functions
 - 7.3. Responsibilities
8. Suspicious Activity & Transactions Reporting
 - 8.1. Confidentiality and Prohibition of Disclosure
9. AML/CTF/CPF Audit
 - 9.1. Independent Audit Function
 - 9.2. Audit Procedures
 - 9.3. Audit Reporting
 - 9.4. Examination by the Gaming Control Board
10. Employee Training & Development
11. Record Keeping
12. Appendices

1. Purpose and Scope of Policy

Pelican Entertainment B.V. has developed a rigorous Anti-Money Laundering / Counter-Terrorism Financing / Counter-Proliferation Financing Policy (referred to as the AML/CTF/CPF Policy) to comply with the standards established by the Curaçao Gaming Control Board, which supervises AML/CTF/CPF adherence in Curaçao. The Board of Directors (BoD) oversees the annual approval, design, implementation, and monitoring of this policy, with an additional mandate to propose updates in response to significant changes in AML/CTF/CPF regulations or company operations. Urgent adjustments may also be initiated by a designated officer following insights from internal or external AML audit findings regarding risk probability and impact.

This policy sets out a structured approach to preventing money laundering, terrorist financing, and proliferation financing. It is applicable to all personnel, counterparties, and third-party consultants, inter alia, and addresses risk factors related to clients, products, services, payment systems, geographic regions, and delivery channels. Aligned with both local and global AML/CTF/CPF standards, the policy reflects key Curaçao legislation, including the National Ordinance for Games of Chance (LOK), the Criminal Code of Curaçao, the National Ordinance on Offshore Games of Hazard (NOOGH), the National Ordinance on Penalization of Money Laundering (NOPML), the National Ordinance on the Reporting of Unusual Transactions (NORUT), the National Ordinance on Identification when Rendering Services (NOIS), and the Sanctions National Ordinance (SNO), along with the Kingdom Sanction Act.

Furthermore, this policy integrates international best practices and frameworks, such as the Financial Action Task Force (FATF) Recommendations, the European Anti-Money Laundering Directives (4th, 5th, and 6th AMLDs), and the Wolfsberg Principles, ensuring a robust compliance posture on all fronts.

2. Online Gaming Environment & Specifics

Pelican Entertainment B.V. is a legally registered entity in Curaçao, holding registration number 134359, registered address Dr. H. Fergusonweg 1, Curaçao, and is the owner and operator of the website:

<https://melbet.com>

melbet.org

<https://astekbet.com/en>

The company operates under a Curaçao online gaming license issued by the Curaçao Gaming Control Board, license number OGL/2024/561/0554, ensuring compliance with licensing obligations and observing regional restrictions enforced by Curaçao's regulatory authorities. These rules prevent remote gaming licensees from offering services in specific

jurisdictions, including the United States, Australia, the Dutch Caribbean (Aruba, Bonaire), Curaçao, France, Germany, the United Kingdom, Belize, and the Netherlands. The company restricts its operations to legally permissible markets and refrains from targeting customers in regions where online gambling is prohibited.

Operators in the e-gaming and betting sector, such as **Pelican Entertainment B.V.**, are exposed to various money laundering risks. These risks include identity theft, fraud, structuring, layering, and collusion between internal employees and customers or third-party payment processors to circumvent internal controls.

3. Assessment of Risks: Money Laundering, Terrorism Financing & Proliferation Financing

3.1. Anti-Money Laundering

Money laundering is a prevalent issue in financial crimes, often spanning international borders and tied to various illicit activities such as tax evasion, sanctions breaches, fraud, corruption, illegal arms trading, drug trafficking, extortion, and kidnapping. Its main purpose is to obscure the criminal origins of assets, effectively masking their source, ownership, and destination as they move through the financial system.

Stages of Money Laundering:

1. **Placement:** The initial step involves introducing illegally obtained funds into the financial system. This could be done by depositing cash into bank accounts, purchasing high-value items, or initiating other financial transactions. This stage aims to start the process of legitimizing illicit money.
2. **Layering:** In this phase, funds undergo multiple transactions designed to conceal their origin, including transferring them across accounts, converting them into different currencies, or investing in various financial instruments. The complexity of these transactions creates a "layer" that makes tracing the origin of funds challenging.
3. **Integration:** At this final stage, laundered funds are reintroduced into the legitimate economy, often by buying luxury items, investing in cash-rich businesses, or engaging in other legal financial activities. At this point, the money appears to have legitimate origins, making it challenging to link it back to its criminal source.

Money laundering may intersect with online gambling sites, highlighting the importance of casinos in preventing anonymous services and identifying suspicious transactions.

Relation to Terrorist Financing:

Terrorist financing entails using funds to support terrorist operations, which can originate from both legitimate and illicit sources but often follow laundering methods to avoid

detection. Common examples include using prepaid cards to purchase items for terrorist purposes. For this reason, staff must be trained in recognizing the latest methods used in terrorist financing.

Risk Management and Compliance:

To manage money laundering risks, the company emphasizes identifying and addressing potential threats through:

- **Fraud and Identity Verification:** Ensuring thorough due diligence, including verifying documentation, age, and location.
- **Monitoring Multiple Accounts and High Transaction Volumes:** Flagging unusual activity involving multiple accounts or high volumes of transactions.
- **Identifying Illicit Deposits:** Detecting and blocking funds suspected of coming from illegal sources or using the platform as a "safe haven."
- **Oversight of Player-to-Player Transfers:** Preventing the misuse of the platform for transferring funds between users or cashing out.

This is not an exhaustive list of potential risks; the company performs tailored risk assessments and provides ongoing training to enhance internal AML compliance.

3.2. Counter-Terrorism Financing

Terrorist financing involves supplying funds for terrorism, originating from either lawful or unlawful sources. This funding enables terrorist activities, which can range from small-scale acts to major attacks.

Key Elements of Terrorist Financing:

- **Funding Sources:**
 - **Legitimate Sources:** Terrorist groups may rely on legitimate revenue streams from businesses, donations, or other lawful activities. For example, donations may be funneled through charities or legitimate business deals to support illicit purposes.
 - **Illicit Sources:** These include money from illegal activities like drug trafficking, fraud, smuggling, and extortion, often laundered to obscure their criminal origins.
- **Transfer Methods:**
 - **Formal Channels:** Terrorist groups may use conventional financial systems, including banks, to move funds. They often employ layering and structuring techniques to avoid detection.
 - **Informal Channels:** Some rely on non-traditional value transfer systems, such as hawala, which operate outside the formal banking system and are harder to track.

Indicators of Terrorist Financing:

- **Unusual Transaction Patterns:** Transactions that deviate from typical business or personal patterns may signal terrorist financing. For instance, frequent transfers to or from high-risk areas or interactions with known terrorist entities are red flags.
- **Suspicious Activities:** Involvement in high-risk industries, large cash deposits, or activities intended to obscure operations can indicate terrorist financing.

Compliance and Regulatory Measures:

- **AML Policies:** Financial institutions and businesses must establish anti-money laundering (AML) measures, including customer due diligence, transaction monitoring, and reporting any suspicious activities.
- **Sanctions Lists:** Companies must screen transactions against sanctions lists, such as those maintained by the Office of Foreign Assets Control (OFAC) or the United Nations Security Council, to prevent inadvertent funding of terrorist activities.

AML Policies and International Standards:

- **Financial Action Task Force (FATF):** FATF sets international standards for combating money laundering and terrorist financing, stressing the need for robust policies to detect and report transactions related to terrorism.
- **Office of Foreign Assets Control (OFAC):** OFAC administers U.S. sanctions related to national security and foreign policy, requiring institutions to block transactions involving individuals or entities on the Specially Designated Nationals (SDN) list.
- **European Union (EU):** EU directives and regulations prevent the misuse of financial systems for terrorist financing, requiring member states to enforce effective AML measures and comply with global sanctions.
- **United Nations (UN):** The UN Security Council issues sanctions and maintains a list of entities associated with terrorism as part of a worldwide initiative to limit terrorist resources.
- **National Regulations:** Many countries enforce AML legislation, including rules to combat terrorist financing. These laws typically mandate financial institutions to perform due diligence, monitor transactions, and report any terrorism-related suspicions.

By implementing these measures, companies and financial institutions help restrict terrorist funding and contribute to global efforts to combat terrorism.

3.3. Counter-Proliferation Financing

Countering Proliferation Financing (CPF) is a key component of international AML/CTF/CPF regulations, designed to prevent financial support for the development and spread of weapons of mass destruction. Under global standards set by bodies like the Financial Action Task Force (FATF), businesses—especially in high-risk sectors like online gaming—are required to implement controls to prevent proliferation financing. This includes customer due diligence (CDD), monitoring transactions for signs of CPF, and screening customers and counterparties against international sanctions lists, such as those maintained by the United Nations and the Office of Foreign Assets Control (OFAC).

In Curaçao, the Gaming Control Board (CGB) mandates that licensed operators follow robust AML/CTF/CPF practices. This includes complying with both local regulations and international requirements, such as the National Ordinance Penalization of Money Laundering (NOPML) and other ordinances regulating unusual transactions and customer identification. Curaçao's gaming legislation requires that operators perform comprehensive risk assessments that encompass CPF risks, particularly when dealing with higher-risk jurisdictions or high-value transactions. The CGB emphasizes that online gaming operators adopt a proactive, risk-based approach that includes regular reviews and updates to compliance procedures to address new and emerging CPF threats, ensuring that their platforms do not serve as channels for proliferation financing.

3.4. Risk-Based Approach

Pelican Entertainment B.V. implements a comprehensive risk-based approach (RBA) to ensure its Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) & Counter-Proliferation Financing (CPF) protocols are effectively prioritized. This approach focuses resources on the highest-priority threats, a necessity given the recent updates in Curaçao's gaming regulations, especially the enactment of the Law on Offshore Games (LOK). This legislation supersedes the former National Ordinance on Offshore Games of Hazard (NOOGH) and introduces stricter AML/CTF/CPF requirements for operators in the gaming sector.

The LOK mandates gaming operators to conduct in-depth risk assessments to better identify and understand specific operational vulnerabilities. For Pelican Entertainment B.V., this means assessing key factors such as customer demographics, transaction behaviors, geographical risks, and the nature of offered services to accurately gauge potential risks of money laundering and terrorist financing.

Additionally, the RBA necessitates continuous risk monitoring and the implementation of effective internal controls. Operators must craft policies that not only meet Curaçao's legal standards but also adhere to global best practices as recommended by the Financial Action Task Force (FATF) and aligned with relevant European Union (EU) directives. These standards underscore the importance of identifying and mitigating risks tied to specific services that could be exploited for financial crime.

Beyond local legislation, Pelican Entertainment B.V. is subject to international regulations aimed at safeguarding financial integrity. The FATF guidelines are designed to prevent the misuse of financial systems, covering areas such as customer due diligence (CDD), transaction monitoring, and reporting suspicious activities.

In line with European Union AML Directives (4th, 5th, and 6th AMLDs), EU-linked jurisdictions like Curaçao are expected to uphold rigorous standards to address money laundering and terrorist financing. To remain compliant, Curaçao must adapt its regulatory structure, ensuring its gaming operators align with EU accountability and transparency standards.

Recent regulatory changes also underscore the importance of countering proliferation financing risks. The company must remain alert to any transactions tied to financing weapons of mass destruction, often linked to broader money laundering and terrorism

financing risks. By adhering to sanctions from bodies like the United Nations Security Council and the Office of Foreign Assets Control (OFAC), Pelican Entertainment B.V. safeguards against inadvertently supporting prohibited individuals or entities.

In summary, Pelican Entertainment B.V.'s adoption of a robust risk-based approach is essential for navigating the complexities of AML, CTF, and CPF. This integrated compliance strategy not only aligns with local and international standards but also reinforces the company's standing in the global gaming market.

3.5. Key Risk Areas Specific to the Gambling Sector

The gambling industry faces unique risks related to money laundering (ML) and terrorist financing (TF). To address these, Pelican Entertainment B.V. evaluates four primary risk areas as part of its business and customer risk assessments.

3.5.1. Distribution Channel Risks

The choice of distribution channel used to establish relationships with clients can significantly impact risk exposure:

- **Anonymous Channels:** Channels that allow for anonymity increase the risk of ML and TF.
- **Non-Face-to-Face Interactions:** Without in-person verification, the likelihood of identity theft or impersonation increases.
- **Third-Party Intermediaries:** When third parties act as intermediaries, especially if they are not subject to AML/CFT laws, they pose additional risks.

Mitigation Strategies for Channel Risks:

- Enforces identity verification for clients, utilizing tools to validate and confirm customer information.
- Prevents impersonation through advanced verification methods and document authentication.
- Restricts relationships with unregulated third-party intermediaries, ensuring all customer interactions meet AML/CFT standards.

3.5.2. Customer Risk

The behavior and characteristics of certain customer types may indicate a higher risk of ML or TF:

- **Multiple Income Sources:** Customers with diverse income sources.
- **Irregular Income:** Those with fluctuating or unpredictable income.
- **Politically Exposed Persons (PEPs):** Individuals with high-ranking public positions.
- **High or Disproportionate Spenders:** Individuals spending large amounts or amounts inconsistent with their income.
- **Casual and Tourist Gamblers:** Those with fluctuating spending habits.
- **Use of Third-Party Involvement:** Intermediaries used to conduct gambling activities.
- **Multiple Casino Accounts:** Customers using numerous accounts to conceal gambling patterns.

- Anonymous Customers: Players redeeming large chips without identification.
- Junket Operators: Intermediaries who monitor players and provide credit.

3.5.3. Mitigation Strategies for Customer Risk:

- Applies standard CDD for all patrons and EDD for high-risk individuals (PEPs, high spenders).
- Continuously updates customer profiles to reflect their current risk levels.
- Employs stringent verification to confirm customer identities.
- Limits third-party transactions to only those that are verified and justified.

3.5.4. Product, Service & Transaction Risks

Certain aspects of gaming services and transactions pose a higher risk due to potential exploitation by criminals:

- Criminal Proceeds: Risks related to money sourced from illegal activities such as fraud, trafficking, or theft.
- Anonymous Payment Methods: Virtual assets or prepaid cards that can obscure the source of funds.
- Casino Accounts for Non-Gaming Use: Accounts used solely for deposits and withdrawals without gaming involvement.
- Peer-to-Peer Gaming: Direct transactions between players.
- Third-Party Account Holders: Where casino account details do not match those of the payment method used.
- Multiple Operators: Situations involving various unlicensed payment systems or e-wallets that obscure beneficiaries.

Company's Risk Mitigation Strategies:

- Verifies customer identities using advanced tools and ensures the accuracy of identification.
- Requires validated source of wealth/funds for transactions above set thresholds, particularly those at or above NAF 4,000.
- Partners only with licensed and regulated payment providers.
- Restricts casino account usage to gaming purposes, overseeing accounts to prevent misuse.
- Controls and monitors peer-to-peer gaming platforms.
- Matches account details with those on payment cards and uses fraud detection tools to prevent identity and other types of fraud.

3.5.5. Geographic Risk

Location-based risks relate to the geographic origin of the customer or their funds. Certain countries present higher risks due to:

- FATF High-Risk Countries: Nations flagged by the FATF for lacking AML/CFT controls.

- Countries Under Enhanced Monitoring: Nations with AML/CFT deficiencies under FATF monitoring.
- CFATF Reports: Countries with region-specific risks noted by the CFATF.
- Sanctions and Compliance Lists: Countries under OFAC sanctions or listed by the U.S. State Department's INCSR.
- Transparency International's Corruption Index: Nations with high levels of corruption are considered high-risk.

3.5.6. Company's Strategies to Mitigate Geographic Risk:

- Maintains an up-to-date list of high-risk countries and reviews locations regularly.
- Monitors and evaluates customer locations based on reliable sources to assign risk ratings.
- Applies enhanced due diligence for customers from high-risk regions, reducing the chance of potential financial crimes.

4. Senior Management Duties & Responsibilities

At Pelican Entertainment B.V., senior management is essential in identifying and managing the inherent risks associated with Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and Counter-Proliferation Financing (CPF). The Board of Directors has designated an AML/CTF Officer tasked with providing regular updates on any significant changes in the control environment. This officer is also responsible for compiling an annual report that assesses the efficacy of the company's systems and controls in addressing risks related to money laundering, terrorist financing, and proliferation financing.

To uphold compliance with local and international standards, senior management is required to conduct thorough reviews of all relevant policies and procedures at least once a year. These reviews are guided by monthly risk assessments, which facilitate the prompt identification of potential vulnerabilities in internal controls and risk management strategies. In cases where deficiencies are noted, the AML/CTF Officer can propose necessary adjustments to the Board for their approval, reinforcing Pelican Entertainment B.V.'s dedication to effective risk management and compliance.

In accordance with best practices globally, senior management must oversee the execution of comprehensive employee training programs. These programs aim to enhance staff awareness and comprehension of AML/CTF/CPF risks, ensuring that all employees, especially those in critical roles, are well-prepared to recognize and react to suspicious activities.

Additionally, senior management is responsible for maintaining a strong internal control framework that includes appropriate segregation of duties, well-defined authorization processes, ongoing monitoring, and meticulous documentation practices. Regular independent audits and evaluations are conducted to objectively assess the effectiveness of

the AML/CTF/CPF program and identify areas for enhancement, ensuring continuous adherence to regulatory requirements.

5. Customer Due Diligence

To comply with regulations, Pelican Entertainment B.V. ensures that all customer accounts are verified and legitimate, without any anonymous or fictitious entries. Accurate player identification and a thorough understanding of each customer relationship are fundamental to reducing the risks of money laundering, terrorist financing, and proliferation financing. An effective Customer Due Diligence (CDD) system is essential for managing risk and ensuring customer activity is aligned with regulatory expectations. Any suspicious behavior must be reported promptly to the Financial Intelligence Unit (FIU) and, if necessary, to the Public Prosecutor's Office.

High-risk transactions automatically trigger Enhanced Due Diligence (EDD) procedures. The Company's anti-fraud system is configured to detect and flag transactions based on specific thresholds, as required by the Gaming Control Board (GCB). These thresholds include:

- Transactions equal to or above NAF 4,000.
- Occasional transactions that exceed NAF 4,000.
- Suspicion of money laundering or terrorism financing.
- Doubts regarding previously provided customer identification information.
- Linked transactions exceeding NAF 4,000 – even when individual transactions are below this threshold, they are flagged if linked.

The Company employs a range of CDD measures to ensure comprehensive identification and monitoring, including:

- **Player Identity Verification:** Verification of player identities is conducted through reliable, independent documents, data, or electronic systems to establish the authenticity of customer information.
- **Ultimate Beneficial Owner (UBO) Identification:** For individual and business accounts, the Company verifies the UBO's identity and examines the ownership structure of any legal entities to ensure transparency regarding the true account holder.
- **Understanding Business Relationship Purpose:** For each customer, the Company assesses the intended purpose and nature of the gaming relationship, which supports a comprehensive understanding of expected activity patterns.
- **Ongoing Monitoring:** Continuous due diligence is conducted on active accounts to ensure transactions align with the customer's profile and declared source of funds when required.

Company staff are instructed to maintain confidentiality around reporting to the FIU. Any knowledge of or suspicion related to money laundering or terrorism financing should not be disclosed to the customer to avoid unintentional tipping-off. In cases where CDD might alert

the customer to the suspicion, the Company refrains from CDD measures and instead files a report directly with the FIU.

5.1. Player Identification & Verification

The Company's identification and verification processes involve collecting essential player information and verifying these details with credible sources. The level of information collected is based on the customer's risk profile.

Player Identification Requirements

At a minimum, the following information is required:

- Full name
- Permanent address
- Date of birth
- Place of birth
- Nationality
- Identification number

For low-risk players, the first three details may suffice. However, for high-risk customers, additional data might be necessary to mitigate ML and TF risks effectively.

Risk-Based Customer Assessment

An initial risk rating is assigned based on basic customer information. This rating may be adjusted as more data is gathered, helping to establish the correct level of CDD as per regulatory requirements.

Verification Methods

Verification of identity involves ensuring that a player is who they claim to be. Acceptable forms of documentation include:

- Government-issued photo ID, such as a passport or national ID card
- Secondary documents, such as utility bills or bank statements, confirming the residential address (no older than six months)
- Verification of address through official correspondence or contact methods, such as phone or email
- Biometric checks, cross-referencing databases, IP addresses, and funding sources

If there are concerns regarding the quality or adequacy of collected information, additional steps are taken. This may involve requesting a selfie with their ID or a first deposit from an account held at a reputable, regulated financial institution.

5.2. Understanding the Purpose and Nature of Business Relationships

As part of the CDD process, the Company establishes the intended purpose and nature of its relationships with players. Although the gaming relationship may appear straightforward, it's important to gather enough information to detect any unusual or suspicious activities.

For high-risk clients, the Company collects documentation on the source of wealth and anticipated activity levels. This allows verification of whether the player's income is legitimate

and sufficient to justify account activity. For lower-risk customers, a declaration of employment, business information, or salary details may be adequate, while higher-risk clients are required to provide documentation from independent, credible sources.

The information gathered is used to model player behavior, support ongoing monitoring, and assist in risk profiling.

5.3. Continuous Monitoring of Identity and Transactions

The Company's AML/CTF/CPF framework ensures ongoing monitoring of player identities and transaction activities to detect and prevent ML/TF risks. This includes periodic updates and verification of player identity details, particularly for high-risk individuals, to confirm their authenticity.

All transactions are reviewed for unusual or suspicious patterns that deviate from established player profiles. Any transaction meeting or exceeding the NAF 4,000 threshold, including linked transactions, undergoes enhanced due diligence. The Company utilizes advanced monitoring systems to flag any red flags in real-time, ensuring timely investigation and reporting to the FIU when required. This approach ensures regulatory compliance while maintaining a safe and transparent gaming environment.

5.4. Enhanced Due Diligence (EDD)

In high-risk cases, the Company applies stringent Enhanced Due Diligence (EDD) measures. EDD is mandated for transactions above NAF 4,000 or where ML/TF suspicion arises. This process involves a thorough review of the player's background, including validation of source of funds and wealth, close examination of transaction patterns, and regular updates of identity information.

For players designated as PEPs, including family members and close associates, EDD includes comprehensive risk assessments and ongoing transaction monitoring. EDD is reinforced with independent, reliable documentation to support the legitimacy of a player's financial activities, ensuring that the Company's operations comply with regulatory standards and protect its integrity.

5.5. Simplified Due Diligence (SDD)

In situations where the risk of money laundering or terrorism financing is minimal, the Company may apply Simplified Due Diligence (SDD). SDD allows for a more streamlined verification process, focusing on basic identification details (such as full name, date of birth, and address). While monitoring remains in place, the frequency and depth of reviews are reduced relative to higher-risk scenarios.

If any unusual activity arises, or the player's risk profile changes, the Company immediately implements enhanced due diligence measures.

5.6. Protocol for Politically Exposed Persons (PEPs)

Due to the heightened risk associated with Politically Exposed Persons (PEPs), the Company's AML/CTF/CPF policy enforces strict procedures for handling relationships with PEPs, their family members, and close associates. Upon identifying a PEP, Enhanced Due Diligence (EDD) is implemented, including obtaining senior management approval before starting or continuing the relationship.

EDD for PEPs involves a thorough understanding of their source of funds and wealth and ongoing transaction monitoring. Regular risk assessments are conducted to detect any unusual activities, ensuring regulatory compliance and protecting the integrity of Company operations.

5.7. Reliance on Third-Party Providers and Technological Tools

When outsourcing elements of the CDD process or utilizing third-party tools, the Company ensures that these entities comply with strict AML/CTF/CPF standards. Before engaging any third-party provider, the Company performs due diligence to confirm that they have robust AML protocols and a solid compliance history.

Third-party providers are audited regularly to verify adherence to AML/CTF/CPF standards, and contracts mandate cooperation with any regulatory inquiries. This ensures the integrity of the Company's AML framework while enhancing security and compliance.

5.8. Termination of Business Relationships

If a customer is found to be involved in suspicious activities or fails to provide adequate information during the due diligence process, the Company reserves the right to terminate the business relationship. This decision must be approved by senior management and documented for regulatory purposes.

Upon termination, the Company thoroughly reviews all account activities, immediately reporting any suspicious transactions to the FIU. Customer access to services is revoked, and account records are retained securely for at least five years, ensuring compliance with retention laws. This vigilant approach helps safeguard against ML/TF risks while aligning with regulatory requirements.

6. Sanctions

Pelican Entertainment B.V.'s AML/CTF/CPF policy enforces strict compliance with both international sanctions and regulatory standards. Our commitment involves establishing and maintaining thorough procedures to ensure all relevant national and international sanctions are upheld. This includes comprehensive due diligence on every client and transaction to prevent interactions with sanctioned individuals, organizations, or locations.

Our policy mandates continuous monitoring, with immediate reporting of any activities that may breach these sanctions. Additionally, regular training is provided to relevant staff,

reinforcing knowledge of current sanctions laws and enhancing compliance across our operations, ultimately preserving the security and integrity of the Company.

The Company ensures all transactions and customer interactions are rigorously screened against the latest Sanctions Lists. This is achieved through automated systems for real-time checks and a constantly updated sanctions database. Should any matches or suspicious activity arise, they are promptly reported to the appropriate authorities. Preventative actions, such as freezing accounts or blocking transactions, are applied to mitigate compliance risks. To stay aligned with regulatory changes, we conduct frequent reviews and updates of our sanctions protocols, fostering a resilient AML/CTF/CPF compliance framework.

The Company's sanctions compliance policy incorporates screenings against various critical lists, including but not limited to:

- **Sanctions National Ordinance (SNO, N.G. 2014, no. 55)**
- **Kingdom Sanction Act (N.G. 2016, no. 54)**
- **Curaçao Gaming Control Board (GCB) Announcements**
- **European Union (EU) Sanctions**
- **United Nations Security Council Consolidated List**
- **United Kingdom OFSI Sanctions**
- **United States List of Foreign Terrorist Organizations**
- **Office of Foreign Assets Control (OFAC) Sanctions**

The Company's due diligence processes are designed to identify any covert or indirect attempts to circumvent sanctions through sanctioned entities or jurisdictions. Should any tactics aimed at sanctions evasion be detected, they will be reported promptly to the relevant authorities. Immediate corrective measures will be implemented, including transaction suspensions and account reviews. Regular audits and targeted staff training programs support ongoing vigilance, ensuring compliance with current legislation and adherence to best practices in detecting and addressing sanctions evasion.

7. Compliance Officer

7.1. Appointment

The Company has designated a qualified individual as the Money Laundering Reporting Officer (MLRO) or Anti-Money Laundering Compliance Officer (AMLCO). This role is vital to the Company's Anti-Money Laundering (AML) framework, and the appointment is made by senior management to guarantee the independence and authority needed to fulfill AML responsibilities effectively. The MLRO/AMLCO is selected based on their relevant experience and expertise in AML compliance and must hold a sufficiently senior position to manage the implementation of AML policies and procedures. This appointment is formalized with an appointment letter, detailing their duties and organizational reporting structure.

7.2. Key Functions

The MLRO/AMLCO oversees essential aspects of the Company's AML program, including:

- Policy Implementation: Ensuring AML policies and procedures are effectively integrated and adhered to across the organization.
- Regulatory Compliance: Confirming that the Company complies with all relevant AML/CTF/CPF regulations.
- Central Contact Point: Serving as the main point of contact for all matters related to AML.

The MLRO/AMLCO also reviews and approves the Company's AML policies to align with current regulatory requirements, oversees the AML training program, and ensures that all employees understand their responsibilities in upholding compliance.

7.3. Responsibilities

The MLRO/AMLCO's core responsibilities include:

- Monitoring and Reporting: Continuously monitoring client activities and transactions to identify and investigate any suspicious activity. The MLRO/AMLCO is responsible for filing Suspicious Activity Reports (SARs) with the Financial Intelligence Unit (FIU) when necessary and keeping comprehensive records of these reports.
- Policy Development: Crafting and updating AML/CTF/CPF policies and procedures to stay in line with Curaçao gaming laws and international best practices. This includes evolving the AML framework to manage emerging risks and regulatory changes.
- Training and Awareness: Ensuring that all employees receive appropriate AML/CTF/CPF training. The MLRO/AMLCO regularly updates training materials to reflect changes in regulations or Company policies, supporting staff in recognizing and reporting suspicious activities.
- Liaison with Authorities: Acting as the Company's primary point of contact with regulatory agencies, law enforcement, and other relevant authorities. This role includes managing information requests and participating in regulatory audits or inspections.
- Compliance Oversight: Conducting regular reviews and audits of the AML/CTF/CPF program to confirm its effectiveness and compliance with legal requirements. The MLRO/AMLCO addresses any issues found during these reviews and ensures corrective actions are implemented as needed.
- Documentation and Record-Keeping: Maintaining detailed records of all AML/CTF/CPF activities, including SARs, internal reports, training, and policy updates. These records must comply with legal requirements and remain readily accessible for regulatory review.

By carrying out these duties, the MLRO/AMLCO plays a central role in protecting the Company against money laundering and terrorist financing risks, ensuring strong compliance with Curaçao's AML/CTF/CPF legislation.

8. Suspicious Activity & Transactions Reporting

The Company is committed to identifying and reporting any unusual activity that could signal potential money laundering or terrorist financing. Unusual activity may include deviations from a client's established behavior, irregular transactional patterns, frequent high-value transfers, or interactions with high-risk regions. Employees are expected to remain vigilant and report any such anomalies immediately to the designated Officer (AMLCO/MLRO). Upon notification, the AMLCO/MLRO conducts a detailed review to assess whether the activity warrants additional measures or reporting to the appropriate authorities.

Unusual transactions are characterized by activity that does not align with the client's known business practices or financial profile. Examples include unexpected large transactions, transactions involving unknown entities, or those without an apparent lawful or economic purpose. Employees utilize transaction monitoring systems to identify these anomalies and escalate them to the AMLCO/MLRO. The AMLCO/MLRO evaluates flagged transactions against specific risk indicators and regulatory standards, ensuring that transactions considered suspicious are promptly reported to the Financial Intelligence Unit (FIU) in line with Curaçao's AML requirements.

8.1. Confidentiality and Prohibition of Disclosure

To uphold the integrity of the reporting process, the Company's policy strictly forbids disclosing any details about suspicious activity reports (SARs) to the individuals involved or unauthorized parties. This confidentiality is essential to prevent interference with ongoing investigations or legal processes. Employees are required to handle all SAR-related communications discreetly, and discussions about SARs are only permitted with the AMLCO/MLRO or authorized personnel. Any breach of this confidentiality policy is regarded as a serious violation of AML/CTF/CPF protocols and may result in disciplinary action. This measure ensures that the reporting process remains confidential and effective in addressing financial crime risks.

9. AML/CTF/CPF Audit

In compliance with Curaçao's updated gaming regulations, the Company undergoes an annual independent audit of its Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) programs. This section details the structure for these audits, the responsibilities of the independent audit function, and the oversight role of the Gaming Control Board.

9.1. Independent Audit Function

The purpose of an annual independent AML/CTF/CPF audit is to evaluate the effectiveness and regulatory compliance of the Company's AML framework. This review ensures the organization aligns with current legal standards and best practices in managing money laundering and terrorist financing risks. The audit scope includes a comprehensive

assessment of the AML/CTF/CPF program, risk assessments, transaction monitoring systems, staff training, and reporting procedures.

Each year, the Company selects an internal or external auditor with adequate resources, AML expertise, and recognized certification. To avoid conflicts of interest, the auditor must operate independently from the Company's AML Compliance team. The selection process considers the auditor's qualifications, experience, and industry reputation, and the chosen auditor must also be approved by the Gaming Control Board to ensure compliance with Curaçao's gaming legislation.

9.2. Audit Procedures

The independent audit follows international auditing standards and specific guidelines from the Curaçao Gaming Control Board. Key procedures in the audit process include:

- **AML/CTF/CPF Policy Review:** Assessing the currency and legal compliance of the Company's policies and procedures.
- **Risk Management Framework Evaluation:** Reviewing the adequacy of risk assessments and mitigation practices.
- **Transaction Monitoring Systems Examination:** Ensuring that systems for detecting and reporting suspicious activities are effective.
- **Staff Training Program Evaluation:** Verifying that training is comprehensive and that employees are equipped to recognize and report suspicious activities.
- **Audit of Reporting Mechanisms:** Reviewing processes for reporting suspicious transactions and regulatory issues.
- **Customer File Review:** Confirming adherence to KYC, KYB, and CDD standards.

These procedures allow the auditor to assess the effectiveness of the Company's AML/CTF/CPF measures and identify any areas requiring improvement.

9.3. Audit Reporting

Upon completing the audit, the independent auditor prepares a report detailing findings, recommendations, and any identified deficiencies. This report is provided to the Company's senior management and submitted to the Gaming Control Board. The Company is then required to address the auditor's recommendations and implement corrective actions within a specified timeframe. Follow-up audits may be scheduled to ensure these measures have been effectively applied.

9.4. Examination by the Gaming Control Board

The Gaming Control Board (GCB) oversees AML/CTF/CPF compliance for all licensed entities, including reviewing independent audit results and conducting its own evaluations. The GCB holds authority to request additional documentation, conduct onsite inspections, and verify that corrective actions from audit recommendations have been implemented.

The GCB examination process includes:

- **Audit Report Review:** Analyzing the independent auditor's findings to assess compliance and identify potential issues.

- **Onsite Inspections:** Conducting site visits to verify the accuracy of audit findings and assess the effectiveness of implemented controls.
- **Interviews and Documentation Review:** Interviewing key personnel and reviewing supporting documentation to gain an in-depth understanding of the Company's AML/CTF/CPF practices.

Entities found non-compliant based on audit or examination findings may face regulatory actions, including fines, operational restrictions, or license suspension or revocation. The Company collaborates closely with the Gaming Control Board to implement corrective actions as needed and to continuously monitor compliance, thus preventing future violations.

10. Employee Training & Development

The Company's AML/CTF/CPF training program is designed to equip employees with the necessary knowledge and skills to identify and prevent money laundering and terrorism financing activities. This training ensures employees understand their legal obligations, recognize suspicious activities, and are familiar with internal procedures for reporting such occurrences. A knowledgeable workforce is vital for enforcing AML/CTF/CPF policies and upholding the integrity and reputation of the gaming sector.

Target Audience for Training

Training is customized based on job functions and is mandatory for all employees, including but not limited to:

- Senior management
- Compliance officers
- Customer-facing employees
- Operational staff
- Other employees involved in financial transactions or customer interactions

All new hires receive AML/CTF/CPF training upon joining the Company, with annual refresher courses provided to all employees. Additional, more frequent training may be scheduled for roles with greater exposure to financial crime risks.

Training Content

The training program covers the following areas:

- Overview of Curaçao's AML/CTF/CPF laws and regulations
- Company's AML/CTF/CPF policies and procedures
- Specific roles and responsibilities in AML/CTF/CPF compliance
- Customer identification and verification (KYC/CDD)
- Detecting and reporting suspicious activities and transactions
- Record-keeping and documentation requirements
- Consequences of non-compliance for individuals and the organization
- Recent trends and typologies in money laundering and terrorism financing

Training Delivery Methods

To maximize effectiveness, training is delivered through a range of methods, including:

- In-person workshops and seminars
- Online courses and webinars
- Interactive e-learning modules
- Case studies and practical exercises
- Role-playing scenarios

Combining these methods helps address different learning preferences and reinforces the training material.

Qualified Trainers

Training is conducted by AML/CTF/CPF compliance experts, either internal compliance officers or external consultants, ensuring that trainers remain current on legal standards and industry best practices. This approach helps maintain the relevance and accuracy of the training content.

11. Record Keeping

The Company adheres to strict AML/CTF/CPF record-keeping protocols to meet regulatory requirements. Comprehensive records, including customer identification, transaction data, suspicious activity reports (SARs), training logs, and audit records, are maintained for a minimum of five years. These records are securely stored with encryption and access controls to prevent unauthorized access, and regular security audits are conducted to ensure data integrity.

Records are organized for easy retrieval to facilitate prompt access by authorized personnel and regulators. Internal reviews and audits are conducted periodically to verify compliance with record-keeping standards. Effective record management is essential for regulatory compliance, supporting audits, and safeguarding the reputation and integrity of the gaming industry.

12. Appendices

Appendix 1: Key Abbreviations

EDD – Enhanced Due Diligence

SAR/STR – Suspicious Activity Report / Suspicious Transaction Report

UN – United Nations

CDD – Customer Due Diligence

SOF/SOW – Source of Funds / Source of Wealth

OFAC – Office of Foreign Assets Control

AML – Anti-Money Laundering
UBO – Ultimate Beneficial Owner
PEP – Politically Exposed Person
CFATF – Caribbean Financial Action Task Force (a coalition of 24 states in the Caribbean Basin, Central, and South America)
NOOGH – National Ordinance on Offshore Games of Hazard (Landsverordening buitengaatsse hazardspelen, P.B. 1993, no. 63)
FIU – Financial Intelligence Unit Curaçao, as per Article 2 of the Norut
KYC – Know Your Customer
UK – United Kingdom
FATF – Financial Action Task Force
US – United States
KYB – Know Your Business
BOD – Board of Directors of the Company
CPF – Counter Proliferation Financing
CTF – Counter Terrorism Financing
Compliance Officer – A senior manager independent from gaming operations, tasked with managing and mitigating ML/TF/CPF risks
EU – European Union

Appendix 2: Key Definitions

Risk Appetite

The level of risk an organization is willing to accept to meet its objectives, helping to guide compliance strategies and allocate resources accordingly.

Suspicious Transaction Report (STR)

A report filed with relevant authorities to document transactions that appear suspicious or deviate from normal activity.

Office of Foreign Assets Control (OFAC)

A division of the U.S. Department of the Treasury responsible for enforcing economic and trade sanctions against specific foreign entities and individuals.

Enhanced Due Diligence (EDD)

Advanced verification measures applied to higher-risk clients to better understand their business activities and financial behavior.

Beneficial Owner

The individual who ultimately holds control over a transaction or account, even if it is registered under another name.

Unusual Transaction

Any transaction that does not align with typical account behavior, potentially indicating an attempt to evade AML detection.

Comprehensive Sanctions

Broad, restrictive measures that prohibit most interactions with a targeted nation or entity, often with few exemptions.

First Line of Defense

The first layer in a compliance program, where employees with direct customer contact gather relevant information for effective screening.

Financial Action Task Force (FATF)

An international organization promoting global standards for AML and counter-terrorism financing, assessing countries and publishing reports on financial crime.

Alert

A notification or warning triggered by AML systems that suggests further review is needed.

The Wolfsberg Group

An association of leading financial institutions that collaborates on anti-money laundering standards and promotes transparency in private banking.

Risk-Based Approach

A strategy for adjusting AML controls based on the specific level of risk presented by customers, products, and transactions.

Know Your Employee (KYE)

Procedures to verify and understand employees' backgrounds and behavior, to identify conflicts of interest or financial crime risks.

Money Laundering Reporting Officer (MLRO)

The official responsible for overseeing the AML program, filing suspicious reports, and managing compliance training.

Automated Screening Tool (AST)

Software designed to automate the process of screening customers, including cross-checks against sanctions lists.

Financial Intelligence Unit (FIU)

A government agency that receives and investigates suspicious transactions, forwarding cases to law enforcement as needed.

Money Laundering

The process of making illicitly obtained funds appear legitimate, usually through placement, layering, and integration.

Know Your Customer (KYC)

Procedures for verifying customer identity and expected behavior, to detect unusual or suspicious transactions.

Criminal Proceeds

Assets or funds obtained through illegal activities, either directly or indirectly.

Customer Relationship

All interactions with a customer, beginning at onboarding and continuing throughout the lifecycle of the account.

Layering

A step in money laundering where illicit funds are moved through multiple transactions to disguise their origins.

Exclusions List

A list that includes names cleared by compliance to avoid future screenings, as they do not match any names on sanctions lists.

Embargo

A government-imposed ban on trade with a specific country or restriction on particular goods.

Suspicious Activity

Any behavior or transaction that deviates from expected patterns and may indicate money laundering or terrorist financing.

Politically Exposed Person (PEP)

A prominent public official or individual with close ties to such individuals, who requires additional scrutiny in financial dealings.

Senior Management

Executives with the authority and responsibility to make decisions affecting the Company's risk of exposure to financial crime.

Due Diligence

A thorough investigation process conducted before entering a business relationship, crucial for identifying risks.

Risk Assessment

A process to identify and evaluate risks that could affect business operations, aiding in developing AML strategies.

Third Line of Defense

The audit function, which independently reviews the effectiveness of controls applied by the first two lines of defense.

High-Risk Third Country

A jurisdiction identified by FATF or other regulatory bodies as having weak AML/CFT controls, posing significant risks.

Sanctions List

A document identifying specific individuals, entities, or countries with whom financial transactions are restricted or prohibited.

Simple Checks

Basic initial steps in an investigation to quickly assess if there is a match with sanctions data.

Regulatory Agency

A government body tasked with overseeing financial institutions, enforcing AML regulations, and conducting examinations.

Egmont Group of Financial Intelligence Units

An international network of FIUs, promoting information sharing and AML expertise across jurisdictions.

Blacklist

An internal list of flagged entities, individuals, or jurisdictions, checked for sanctions exposure along with official sanctions lists.

Minor

An individual under the legal age of majority, typically 18.

Inherent Risk

The baseline level of risk present before applying any mitigation measures.

Embargo

An official ban on trade with a country, often applied to goods like oil or other resources.

Economic Sanctions

Restrictive measures imposed by one or more countries to influence foreign policy or behavior.

Sanctions Due Diligence (SDD)

Due diligence specifically targeting sanctions risks, building on KYC information, and applied continuously throughout the customer relationship.

Third-Party Database

An external data source, such as credit agencies or other legal databases, for additional verification of customer information.

Customer

An individual who opens an account and engages in financial transactions with the Company.

Sanctions Compliance

The process of adhering to laws and regulations regarding sanctions, ensuring the organization meets all compliance requirements.

Greylist

A list of jurisdictions or entities flagged as having deficiencies in AML controls, with ongoing efforts to address them.

Investigation

A detailed process of gathering information in response to potential financial crime alerts, often beginning with basic checks.

Structuring

The act of splitting large transactions into smaller amounts to avoid triggering AML or reporting thresholds.

Sanctions Regime

A coordinated set of restrictions with a shared policy goal, which may involve both unilateral and multilateral sanctions.

Red Flag

An indicator or warning sign that suggests a potential financial crime risk or unusual activity.

Sanctions Evasion

The intentional act of concealing the involvement of sanctioned parties to bypass restrictions.

European Union (EU)

A political and economic union that mandates AML and CFT compliance within its member states, providing regular regulatory updates.

Comprehensive Sanctions

Strict restrictions that generally prohibit all transactions with a sanctioned entity or country.

First Line of Defense

The initial point in a compliance framework, where customer-facing employees gather essential KYC information.

Sanctions

Legal restrictions aimed at preventing financial dealings with specific individuals, entities, or countries.

United Nations (UN)

An international organization that promotes global security and includes AML initiatives, like the Global Program against Money Laundering (GPML).



(SMES) Solutions for Management
and Employment Support N.V.

Director

Date: 05.12.2024