

Pelican Entertainment B.V.

(Reg. No: 134359)

AML/CTF/CPF Policy, Sanctions Policy, and Client's acceptance policy

Version 1 Approved on December 5, 2024	By the Board of Directors
Version 2 Approved on May 26, 2025 Appointed Compliance Officer Melanya Sargsyan compliance@pelicanbv.com	By the Board of Directors
Version 3 Approved on December 19, 2025 Appointed Compliance Officer Melanya Sargsyan compliance@pelicanbv.com	By the Board of Directors

Next Scheduled Review: December 2026



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

Managing Director

22.12.2025

1. Purpose and Scope of Policy

Pelican Entertainment B.V. (“the Company” “we”, “our”) 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 Authority, 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 the best international 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.

As of May 15, 2024, new regulatory requirements governing the prevention of money laundering, terrorism financing, and the proliferation of weapons of mass destruction became applicable to Curaçao-licensed online operators, with full enforcement commencing September 1, 2024. Failure to comply may result in serious administrative or criminal sanctions, demonstrating the heightened regulatory expectations placed upon the industry. These updated AML/CFT/CPF regulations are fully aligned with FATF standards and the broader legislative framework in Curaçao.

In summary, Pelican Entertainment B.V.’s AML Policy has been developed to meet and exceed the expectations of the Curaçao AML/CFT supervisory authority, the Curaçao Curaçao Gaming Authority (CGA). All company directors, officers, employees, and approved third-party auditors are required to adhere to the standards set out in this Policy

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 Authority, 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 Authority (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.

3.6 Risk Areas Specific to Gambling Sector

Technological Developments Risk Assessment

Pelican Entertainment B.V. maintains appropriate procedures and controls for identifying and mitigating risks associated with technological innovations. A documented risk assessment shall be conducted whenever a new product, delivery method, or technology is introduced. This includes pre-launch assessments to evaluate if any vulnerabilities exist that could be exploited for money laundering or terrorist financing. Identified risks must be addressed through enhanced controls, and findings shall be documented and reviewed annually.

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. Risk-Based Compliance Framework

A core pillar of **Company**'s compliance framework is its structured risk assessment process, built around a **risk-based approach (RBA)**. This approach involves systematically evaluating risks related to customer profiles, products, services, transaction types, and geographic exposure. The goal is to proactively identify and address potential vulnerabilities before they can impact operations. Through ongoing assessments, Company enhances its ability to detect, assess, and respond to emerging financial crime threats while maintaining full alignment with Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) obligations.

Implementation of Risk Mitigation Controls

Once risks are identified, Company applies tailored mitigation strategies based on the level and type of risk exposure. These strategies form the foundation of its financial crime prevention efforts, enabling the company to counter threats such as money laundering, terrorism financing, and proliferation financing.

A key component is Enhanced Due Diligence (EDD)—a more rigorous review process for high-risk customers and transactions. This includes detailed assessments of the source of funds, verification of beneficial ownership structures, and scrutiny of financial histories. These procedures are essential in detecting hidden financial risks and blocking illicit financial flows.

Company also deploys real-time transaction monitoring systems, which use automated alerts to flag suspicious activity patterns—such as sudden large deposits or unusual transfer behaviors. Custom alert thresholds enable swift reviews and investigations of potentially illicit activities.

Customer verification is further reinforced through robust identity checks, especially for high-risk clients. This includes verification against trusted data sources and continuous monitoring for red flags. These steps ensure only verified individuals can engage in financial transactions on the platform.

5.1 Risk Assessment Scoring

Money laundering and terrorist financing risks are measured by using a number of factors listed above. Pelican Entertainment B.V. uses the application of risk categories to clients/situations to provide a strategy for managing potential risks and it enables the Company to subject clients to proportionate due diligence and ongoing monitoring. The weight given to these criteria in assessing the overall risk of the client and risk score assigned is as follows:

Category	Score	Level of Due Diligence	Approval Process
Low Risk	0-1.5	Standard Due Diligence	Client Service/Compliance Officer
Medium Risk	1.5.-3.5	Standard Due Diligence	Client Service/Compliance Officer
High Risk	3.5 or more	Enhanced Due Diligence	Annual and approval from Compliance Officer
Unacceptable	Any of the factors that are not accepted by the company	Automatically Reject	Automatically Reject

Risk Scoring and Due Diligence Requirements

A client's Risk Score determines the level of due diligence required and identifies which parties within Pelican Entertainment B.V. are responsible for conducting it. Regardless of the assigned risk rating, Pelican Entertainment B.V. performs automated PEP, sanctions, and adverse media screening on all clients as part of both initial due diligence and ongoing monitoring, ensuring full compliance with regulatory obligations.

The Risk Score also guides how the Company approaches identification, verification, additional information requests, and ongoing monitoring, as outlined below:

Low Risk Standard Due Diligence (SDD)

Clients assessed as low risk pose minimal overall risk to the Company. However, due to the inherently high-risk nature of online gambling, Pelican Entertainment B.V. does not apply Simplified Due Diligence under any circumstances.

Medium Risk Standard Due Diligence (SDD)

Clients categorized as medium risk require the standard level of due diligence and monitoring. Their profiles present moderate exposure, but not enough to warrant enhanced measures.

High Risk Enhanced Due Diligence (EDD)

High-risk clients require Enhanced Due Diligence, conducted and approved by the Compliance Officer. These clients are subject to additional scrutiny and may be accepted or rejected following a formal review and final sign-off.

High-risk classifications may result from, but are not limited to, the following situations:

- The business relationship is conducted in unusual or atypical circumstances.
- Transactions are complex, unusually large, or inconsistent with the client's known profile or peer group.
- The client resides in a high-risk or sanctioned jurisdiction.
- The client is identified as a Politically Exposed Person (PEP), or is a family member or close associate of a PEP.
- The client receives a high-risk score at onboarding (see Player Risk Scoring Assessment, **Appendix I**).
- High-risk indicators arise due to combined risk factors, such as adverse media, unusually large deposits, or suspicious transactional behavior.
- The client provides false, altered, or stolen identification documents or other misleading information.
- Transactions appear to have no legitimate economic or legal purpose.
- The client represents a company offering financial services or services to underlying clients, except licensed liquidity providers.
- The client's lifetime deposit amounts exceed expected thresholds when combined with other risk indicators.

Prohibited Clients

Pelican Entertainment B.V. does not establish or maintain business relationships with clients who fall into prohibited categories, including:

- Individuals or entities subject to financial sanctions or known to have engaged in money laundering or terrorist financing.
- Any person listed on sanctions registers, as Pelican Entertainment B.V. must strictly comply with all applicable sanctions regimes.
- Individuals under 18 years of age. All minors are automatically rejected at onboarding.
- Individuals with unknown or unverifiable sources of wealth or funds.
- Clients whose gameplay or transactional behavior matches known fraudulent or abusive patterns.

6. Continuous Monitoring

Pelican Entertainment B.V. is obliged to conduct ongoing monitoring of business relationships with their clients. Compliance Team conducts ongoing monitoring of clients in the following ways in accordance with the Company's risk-based approach:

Screening of clients against PEP, Sanctions, and Adverse Media on a regular basis. Any alerts considered to be true matches may trigger an Event-Driven Review.

i. Event-Driven Reviews

Certain events will trigger an Event-Driven Review which may, depending on the type of changes flagged, require a full customer due to diligence refresh.

Pelican Entertainment B.V., through the course of its daily activities, obtains the information that brings a question to the accuracy of the customer due diligence information collected, or if suspicion arises, then the customer will undergo an immediate review, irrespective of their risk status.

ii. Periodic Reviews

Pelican Entertainment B.V. has an obligation to ensure that customer due diligence information is relevant and kept up to date via regular client reviews. The extent to which clients' reviews are undertaken will be determined by using a risk-based approach and applied in accordance with the risk rating applied to the customer during the customer risk assessment. The Company has a customer review process based on the High, Medium, and Low risk factors assigned to its customers

The periodic reviews are conducted in line with the client's risk score and profiles are as follows.

High Risk – Every year. This will entail establishing the following:

- Re-confirmation of Address
- Re-confirmation of Source of Funds and Wealth
- Screening for adverse news
- Complete review of transaction profile, including new products requested

Medium Risk – Every two years. This will entail establishing the following:

- Re-confirmation of Address
- Re-confirmation of Source of Funds and Wealth
- Screening for adverse media
- Complete review of transaction profile, including new products requested

The information obtained during the review will be assessed to determine if the medium risk rating still applies.

Low Risk – Every three years. However, reviews will be undertaken when trigger events occur such as:

- where the firm had come into possession of news or information that brings doubt to the accuracy of the current CDD information held
- when the Firm has identified activity deemed to be suspicious
- This review will entail establishing the following:
 - Re-confirmation of Address
 - Screening for adverse media

- The information obtained during the renewal will be assessed to determine if the low-risk rating still applies.

The company's procedures are reassessed whenever the National Risk Assessment (NRA) is updated, ensuring that internal controls, risk ratings, and related measures remain aligned with current national risk priorities and regulatory expectations. Confirm procedures are reassessed whenever the NRA is updated.

• Risk- Driven Approach

Company applies a risk-based approach in combating exploitation of its online platform for the purposes of ML and TF. The methodology the Company adopts is based on the Guidance of the Financial Action Task Force (FATF) as regards ML/ TF Risk Assessments and determines a risk level by evaluating types of risk, threats, vulnerabilities, controls, consequences, the likelihood of it happening, and the impact it may have on the business model in a particular geographical location.

Pelican Entertainment B.V. conducts a formal Business Risk Assessment (BRA) annually and upon any significant operational change. This BRA evaluates money laundering and terrorism financing risks associated with clients, products, delivery channels, geographical exposure, and technological developments. The assessment is documented, approved by the Board of Directors, and revised in accordance with the latest regulatory updates or business model changes

Specifically, AML/CFT risk assessment categories center around the risks associated with:

Risk Indicators

Client risk pertains to the likelihood of exposure to money laundering (ML) and terrorism financing (TF) through interactions with particular individuals. As part of its risk-based compliance model, Pelican Entertainment B.V. conducts thorough evaluations of client profiles, financial transactions, and sources of wealth to identify potential vulnerabilities.

Certain client types are considered to carry a higher risk of financial crime involvement. This includes individuals with multiple income streams, which can complicate the verification process of fund legitimacy. Clients with fluctuating or unpredictable financial behavior may also increase the risk due to the challenge in assessing their financial patterns. Politically Exposed Persons (PEPs) are subject to intensified scrutiny owing to their potential influence over public funds and associated corruption risks.

Additional high-risk categories include individuals with substantial and inconsistent spending, whose expenditures appear disproportionate to their declared income, and clients who maintain multiple gaming accounts, potentially to evade monitoring or obscure financial activity. To address these risks, Pelican Entertainment B.V. has implemented transaction thresholds that reflect normal client behavior patterns.

Typically, low-risk individuals are characterized by having a single, verifiable source of income. In contrast, those with multiple income sources, inconsistent spending patterns, or irregular transactions are subject to elevated monitoring and Enhanced Due Diligence (EDD) measures.

Risks Related to Products, Services, and Transactions

Certain gaming services, financial instruments, and transaction types inherently present greater risks of being exploited for money laundering and terrorism financing. Criminal actors often target weak points within gaming ecosystems to manipulate outcomes or obscure the origins of illicit proceeds.

Illicit funds derived from activities such as fraud, narcotics trade, or theft may be funneled through gambling platforms to disguise their origin. The use of anonymous payment tools such as prepaid cards and digital assets like cryptocurrencies or tokens presents heightened risks due to limited traceability.

The misuse of player accounts for non-gaming purposes, such as acting as temporary repositories for financial transactions, also raises compliance concerns. Similarly, peer-to-peer transfers among players can facilitate unauthorized movement of funds.

Criminals may attempt to exploit third-party financial instruments, such as bank accounts or cards registered under different identities, or transfer funds across multiple gaming accounts, further complicating traceability. Financial services linked to gambling, such as currency exchanges, credit facilities, or use of multi-operator platforms, present an additional layer of risk.

To counter these threats, Pelican Entertainment B.V. enforces stringent transaction monitoring protocols, applies EDD processes where appropriate, and maintains full compliance with global AML/CTF/CPF regulations.

Criteria Used to Assess Transaction Risk:

- Account monitoring (deposit, withdrawals and account activity)
- Transaction monitoring (activity and analysis screening results for deposits and withdrawals)
- Transaction monitoring to track specific patterns in client' activities and detect fraud

Criteria Used to Assess Product or Service Risk:

- Risk typologies associated with each product or service
- The level of transparency, or opaqueness, the product, service, or transaction affords
- The complexity of the product, service, or transaction
- The value or size of the product, service, or transaction

Geographical Risk

Geographical risk is determined by the location of a client and the origin of their financial resources, which may indicate elevated exposure to ML, TF, or Counter-Proliferation Financing (CPF) threats. Jurisdictions associated with weak AML/CFT controls, high corruption levels, or international sanctions pose heightened risk. Countries identified in relation to terrorism or weapons proliferation are subject to strict oversight.

To evaluate such risks, Pelican Entertainment B.V. relies on reputable regulatory and international data sources, including but not limited to:

- Reports from the Financial Action Task Force (FATF), identifying high-risk countries under increased monitoring;
- Caribbean Financial Action Task Force (CFATF) public statements concerning regional financial crime issues;
- U.S. Department of State International Narcotics Control Strategy Reports (INCSR), highlighting financial crime trends;
- The European Commission's list of high-risk third countries with AML/CFT deficiencies;
- Office of Foreign Assets Control (OFAC) sanctions lists targeting terrorism-linked jurisdictions;
- Transparency International's Corruption Perceptions Index (CPI), which ranks countries based on perceived levels of corruption.

Pelican Entertainment B.V. applies a structured geographic risk classification methodology to differentiate between high-risk and low-risk countries. Enhanced Due Diligence is employed for users in higher-risk jurisdictions, and financial activity involving sanctioned territories is restricted. Risk classification protocols and monitoring systems are continuously updated to reflect changes in global assessments, ensuring ongoing compliance with AML/CTF/CPF regulations and maintaining a secure, transparent operating environment.

Risks Associated with Distribution Channels and Their Mitigation Measures

The methods by which Pelican Entertainment B.V. engages with its clients also introduce potential exposure to money laundering, terrorist financing, and fraudulent activity. Channels that facilitate anonymity particularly those enabling financial transactions or user interactions without proper identification pose increased risk if not appropriately controlled.

To mitigate these vulnerabilities, the company enforces advanced verification measures for all client interactions involving anonymous features. Technological solutions, including biometric authentication and sophisticated identity verification tools, are employed to reduce risks associated with fraud and unverified transactions.

By applying rigorous monitoring procedures and ensuring secure authentication across all distribution points, Pelican Entertainment B.V. reinforces its commitment to international compliance standards and strengthens the security and transparency of its gaming platform against financial crime threats.

Factors considered to evaluate Delivery Channel Risk:

- Whether the Company with the client conducted on a non-face to face basis
- Whether the Company personally knows the customer and conducts business on face-to-face basis
- Client not known by the Company but well known in the industry and came to the Company by trusted sources

Assessment of Risks from Technological Developments

Prior to the launch of any new technology, digital product, delivery method, or operational process, Pelican Entertainment B.V. conducts a formal and documented technological risk assessment. This process is mandatory and forms a core component of the Company's risk-based approach to AML/CTF/CPF compliance.

The risk assessment must be:

- Completed and reviewed prior to deployment, ensuring no new technology is introduced without first understanding its vulnerabilities and potential misuse.
- Fully documented in writing, including details of the product or system being assessed, identified risks, mitigation measures, residual risk levels, and decision-making rationale.
- Retained in internal compliance records and made available to the Curaçao Gaming Authority upon request.

Documented assessments are required for:

- New gaming platforms, digital tools, or payment channels.
- Any update to existing infrastructure that significantly changes risk exposure.
- The use or integration of AI systems, blockchain, or third-party services.

- Innovations involving anonymous payment mechanisms or remote account access.

This approach ensures all technological advancements are introduced responsibly, with due consideration for AML/CTF/CPF risks and are aligned with the supervisory expectations of the GCB.

Pelican Entertainment B.V. is dedicated to ensuring that advancements in technology are not exploited for the purpose of financial crimes such as money laundering (ML) or terrorist financing (TF). As innovation continues to transform the iGaming sector, the company implements robust controls and a proactive risk management framework to identify and mitigate any vulnerabilities associated with technological change. Through the integration of thorough risk evaluation processes, Pelican Entertainment B.V. safeguards its compliance obligations across all new business practices, service models, and product innovations.

Procedures for Risk Identification and Assessment

In order to detect and manage risks associated with technological innovation, Pelican Entertainment B.V. conducts in-depth assessments in the following scenarios:

- The launch of a new product or feature on the gaming platform;
- The introduction of operational practices aimed at improving efficiency or enhancing user engagement;
- The adoption of novel service delivery mechanisms, including modern payment technologies or digital account access tools;
- The deployment or integration of emerging technologies into current or future gaming infrastructure, such as blockchain solutions, AI-powered services, or advanced cybersecurity protocols.

Prior to implementing any new technology, a comprehensive review is conducted to assess potential vulnerabilities that could be exploited for criminal activity. This process involves identifying and analyzing associated risks and ensuring all findings are thoroughly documented. The assessment is aligned with both domestic and international AML/CTF regulatory frameworks, reinforcing the company's ability to identify, manage, and mitigate technology-driven threats related to financial crime.

Execution of Risk Mitigation Strategies

Upon identification of potential risks, Pelican Entertainment B.V. promptly adopts appropriate mitigation measures to reinforce its defenses against emerging threats. These may include:

- **Strengthening of Security Protocols** – The implementation of multi-factor authentication (MFA), biometric identity verification, end-to-end data encryption, and artificial intelligence (AI)-based fraud detection tools to safeguard systems from misuse;
- **Enhancement of Transaction Monitoring Capabilities** – Upgrading monitoring platforms to detect atypical financial behavior using automated systems capable of flagging transaction patterns indicative of ML or TF;
- **Policy Adaptation** – Revising AML/CTF policies to address new risk factors introduced by evolving technology. The company ensures that its compliance framework remains agile, keeping pace with the dynamic nature of cybercrime and financial crime techniques.

Through ongoing monitoring and adjustment to technological developments, Pelican Entertainment B.V. upholds its commitment to maintaining a secure and compliant operational environment. This forward-looking strategy protects the integrity of the company's financial ecosystem and affirms its alignment with global

AML/CTF obligations. By doing so, the company ensures that innovation is not pursued at the expense of regulatory compliance or financial security.

Based on the analysis of the risk indicators, the risk model calculates a risk rating of low, medium or high which is then used to create a risk profile which is then assigned to the players and payment service providers at the onboarding stage and is reassessed and amended during the business relationship within the framework of periodic KYC/KYB reviews. Online casinos possess inherent high risks, so the Company strives to rely on its AML and Anti-Fraud key personnel to maintain effective internal controls and CDD measures as reflected in relevant policies.

Industry-Specific Risks in iGaming

Given the specific vulnerabilities within the online gambling industry Pelican Entertainment B.V. has tailored its compliance controls to meet the challenges unique to the sector. Gambling platforms can be exploited to obscure the origin of funds, particularly through layered betting patterns, rapid fund turnover, and irregular payout behaviors. Criminals may use these tactics to convert illicit funds into seemingly legitimate winnings.

To counteract this, the company ensures that all deposits and withdrawals are routed exclusively through licensed financial institutions. Payments using anonymous or untraceable instruments, such as certain cryptocurrencies or unregistered prepaid cards, are restricted or entirely prohibited. Monitoring tools have been configured to detect unusual betting patterns, excessive deposit frequency, and sudden withdrawals that deviate from typical gaming behavior.

Employee training plays a vital role in strengthening the company's overall risk posture. Compliance staff and client-facing teams are routinely trained to recognize red flags, report suspicious activity, and stay informed of evolving criminal methodologies within the gambling landscape.

The ML/FT/FP Policy is designed to combat money laundering and the financing of terrorism, uphold the highest industry standards, and maintain compliance with both domestic and international ML/FT/FP regulatory frameworks. This policy establishes a unified, risk-based methodology that rigorously addresses threats associated with customers, products and services, payment systems, geographic regions, and distribution channels.

It is aligned with key global anti-money laundering and counter-terrorism financing objectives and complies with the prevailing legislative framework in Curaçao. This includes the National Ordinance for Games of Chance (LOK), the Criminal Code of Curaçao, the National Ordinance on Offshore Games of Hazard (PB 1993, no. 63) (LOK), the National Ordinance on the Penalization of Money Laundering (NOPML), the National Ordinance on the Reporting of Unusual Transactions (NORUT, N.G. 2017, no. 99) with amendments effective May 16, 2024, and the National Ordinance on Identification when Rendering Services (NOIS, N.G. 2017, no. 92) with its corresponding 2024 amendments. It also references the Sanctions National Ordinance (SNO, N.G. 2014, no. 55) and the Kingdom Sanctions Act (N.G. 2016, no. 54).

Furthermore, the policy integrates internationally recognized standards and frameworks such as the Financial Action Task Force (FATF) Recommendations, the 4th, 5th, and 6th European Union Anti-Money Laundering Directives (AMLDs), and the Wolfsberg Group Principles.

Risk Mitigation Actions

When a risk is identified whether at the client, transaction, jurisdictional, or service level, Pelican Entertainment B.V. responds with tailored mitigation strategies. EDD is applied to higher-risk profiles, requiring additional documentation and background checks. The company collects detailed information on the source and intended use of funds, while conducting ongoing screenings against global sanctions lists and watchlists.

Sophisticated transaction monitoring systems operate continuously in the background, equipped with real-time alerting capabilities. These systems analyze transaction flow and behavior to detect anomalies, flagging them for internal review. Alerts generated are triaged and, when necessary, escalated for formal investigation and reporting to the Financial Intelligence Unit (FIU).

To protect against identity fraud, strict verification processes are enforced. These include cross-referencing client data against sanctions databases, screening for duplicate accounts, and performing regular updates to maintain the accuracy of stored information.

Oversight, Policy Adjustment, and Reporting

Pelican Entertainment B.V. understands that financial crime risks are dynamic, requiring constant vigilance. To ensure our controls remain effective, we conduct periodic internal reviews of transaction activity, client risk ratings, and compliance procedures. These findings inform policy updates and the adaptation of monitoring tools, ensuring alignment with both regulatory changes and emerging criminal tactics.

All suspicious transactions are promptly reported to the appropriate authorities in accordance with regulatory obligations. Record-keeping is maintained at a high standard covering client onboarding details, transaction data, risk classification documentation, and due diligence records for the required legal retention period. These records are securely stored and made available for inspection during audits or regulatory reviews, reflecting the company's commitment to transparency and accountability.

Comprehensive Risk Governance

Through this holistic and risk-focused compliance strategy, Pelican Entertainment B.V. demonstrates its commitment to preventing financial crime within the iGaming sector. By integrating compliance into every level of operations from onboarding to transaction oversight the company ensures that it not only complies with Curaçao's AML/CTF/CPF requirements but also contributes to the integrity and trustworthiness of the broader financial system.

Risk Assessment Documentation and Accessibility

Pelican Entertainment B.V. maintains a comprehensive Business Risk Assessment (BRA) and Customer Risk Assessment (CRA) in accordance with the requirements set out in the Curaçao Gaming Authority AML/CTF/CPF Regulations. These assessments are structured, evidence-based, and tailored to the nature, size, and complexity of the company's operations and customer base. The BRA identifies and evaluates inherent risks associated with products, services, delivery channels, geographic exposures, and customer segments, while the CRA is used to determine individual customer risk ratings based on factors such as source of funds, transaction behavior, jurisdiction, and PEP status.

The BRA and CRA are developed using a risk-based methodology, updated regularly to reflect changes in risk exposure, and used to inform the implementation of proportionate control measures across the business. These documents are retained in written form and are made available to the Curaçao Gaming Authority or other competent authorities immediately upon request.

7. Guidelines for Client Due Diligence (CDD, EDD) and Client Acceptance Policy (CAP)

When establishing a business relationship, it is essential for Pelican Entertainment B.V. to determine whether a prospective client poses any risk of money laundering, terrorist financing, or proliferation financing within its online ecosystem. **Client Due Diligence (CDD)** forms the foundation of the Company's risk-based approach, supporting the risk-scoring process through the assessment of behavioral indicators, transactional patterns, client profiles, and product- or service-specific risk factors.

Within the AML context, CDD is a structured procedure that includes identifying the prospective client, verifying their identity and age, gathering supplementary information to build an accurate economic profile, assigning a risk rating, and continuously monitoring behavioral and transactional activity for any anomalies that may indicate non-compliance with AML/CFT laws or internal policies.

Open-source intelligence tools such as social-media reviews, property-ownership checks, employment verification, and insolvency searches may be used to support the CDD process where appropriate.

CDD measures may be streamlined when the initial data indicates that the client poses a **low level of risk**.

Conversely, **Enhanced Due Diligence (EDD)** is applied when additional scrutiny is required, such as in cases involving politically exposed persons (PEPs), clients from high-risk jurisdictions, or other risk indicators flagged by the system.

Pelican Entertainment B.V. created a risk scoring system by categorizing clients in accordance with set risk profiles which are construed from the physical location of the clients, their transactional behavior and the products they use. The integrity of the Pelican Entertainment B.V.'s gaming environment is maintained through the application of protocols based on utilizing advanced technology and third-party databases including a proprietary anti-fraud system for onboarding and transaction monitoring, artificial intelligence tools (AI), biometric identification in some instances and RegTech screening tools such as WorldCheck, LexisNexis, SEON etc.

The company is dedicated to maintaining compliance with regulatory standards that prohibit the establishment of anonymous or fictitious accounts within the casino sector. To effectively combat risks related to money laundering, terrorist financing, and proliferation, it is imperative to verify player identities and comprehend their business relationships. A comprehensive Client Due Diligence (CDD) policy is essential for evaluating risks and ensuring adherence to all regulatory obligations. Any activities deemed suspicious will be reported to the Financial Intelligence Unit (FIU) and, if necessary, to the Public Prosecutor's Office.

A Client Acceptance Policy (CAP) has been established to categorize players into low, medium, and high-risk profiles based on geographical location, transaction behavior, income source, and other factors. The CAP outlines enhanced due diligence measures and specifies scenarios where services will be denied due to elevated ML/TF risk. For more detailed information please refer to the **Appendix IV (Client Acceptance Policy)**.

8. The company implements CDD measures

Transactions of NAF 4,000 or more: CDD measures are applied to any single transaction that meets or exceeds this threshold.

Occasional transactions exceed NAF 4,000: This includes infrequent transactions that surpass the specified limit.

Suspicion of illicit activities: Any indication of money laundering or terrorist financing will trigger CDD protocols.

Uncertainties in client identification: If previously obtained identification data raises doubts, CDD measures will be activated.

Linked transactions: This applies to either a single transaction or multiple transactions that collectively exceed NAF 4,000. Even if individual transactions are below this threshold, linked

transactions will still necessitate CDD. High-risk transactions will require Enhanced Due Diligence (EDD).

The company's CDD procedures will encompass the following actions:

Identity Verification: Players will be identified using credible, independent documents or data. This process includes confirming the ultimate beneficial owner of legal entities and understanding their ownership structure.

Ongoing Monitoring: Continuous due diligence will be conducted to monitor transactions, ensuring alignment with the company's understanding of the player and their risk profile, including the source of funds as needed.

Confidential Reporting: Employees are instructed to maintain confidentiality regarding reports made to the FIU, thereby preventing players from being alerted. If suspicions of money laundering or terrorist financing arise, the company will bypass standard CDD processes and report directly to the FIU.

To confirm a player's identity, the company will collect the following details:

- Full name
- Permanent residential address
- Date of birth
- Place of birth
- Nationality
- Identity number
- For low-risk scenarios, only basic information will be required. In higher-risk situations, more detailed information will be collected to mitigate the risks associated with money laundering and terrorist financing.
- Risk Evaluation: Players will be assigned initial risk ratings based on collected information, which will be revised as more data becomes available to determine the appropriate level of CDD.
- Verification Methods: Identity verification will be executed through:
 - Government-issued photo identification (e.g., passport or ID card).
 - Supplementary documents (e.g., utility bills or bank statements) confirming the address, dated within the last six months.
 - Verification of the address through communication methods such as letters, email, or phone.
 - Biometric checks, cross-referencing database information, IP addresses, and funding methods.
- If initial information is insufficient, further verification steps may include requesting a selfie with the ID or confirming the first deposit through a regulated financial institution.

The company will seek to identify the purpose and nature of its relationships with players as part of the CDD process. While some relationships may be clear, the company will gather sufficient information to detect any unusual or suspicious activities. For higher risk

clients, detailed documentation of their source of wealth and expected activity levels will be collected to ensure legitimacy. For lower and medium-risk players, basic employment or business information will suffice, supplemented by independent verification for higher-risk individuals.

9. Timing for Applying Client Due Diligence Measures

Pelican Entertainment B.V. enforces the timely implementation of Client Due Diligence (CDD) procedures to ensure full compliance with applicable Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) regulations. These procedures are designed to proactively identify and verify clients in accordance with regulatory requirements and internal risk assessments.

CDD Triggered by Transaction Thresholds

At the point of account registration, Pelican Entertainment B.V. collects and verifies core client information, including full legal name, permanent residential address, and date of birth. Additionally, clients undergo Politically Exposed Person (PEP) screening and are cross-checked against relevant sanctions lists to ensure they are not linked to prohibited or high-risk entities.

In line with the company's risk-based approach, full identity verification is completed prior to processing any financial transaction that reaches or exceeds the threshold of NAF 4,000. This requirement applies to both individual transactions and cumulative transactions such as multiple deposits, withdrawals, or player-to-player transfers that collectively meet the threshold within a relevant time frame.

Pelican Entertainment B.V. actively monitors all financial activity on a continuous basis. Transaction data is aggregated daily to ensure that the cumulative behavior of each player is considered when assessing risk exposure and determining the need for additional due diligence.

When the threshold of NAF 4,000 is met, the company conducts a comprehensive client risk assessment. This includes reviewing all previously collected information, completing any outstanding CDD obligations, and updating the client's risk classification as needed.

Early Application of CDD Procedures

As a proactive measure, Pelican Entertainment B.V. aims to complete CDD procedures at the earliest opportunity preferably during account registration regardless of whether a financial threshold has been reached. By verifying client identities prior to their participation in financial transactions, the company reduces the likelihood of criminal actors exploiting the platform before thorough due diligence has been conducted

Temporary Limitations Pending CDD Completion

In circumstances where a client reaches the NAF 4,000 threshold before completing full CDD verification, Pelican Entertainment B.V. applies specific transactional restrictions to preserve regulatory compliance:

If the threshold is met due to a deposit, the client is prevented from making further deposits or withdrawals. However, they may continue using existing funds for gameplay activities.

If the threshold is reached due to a withdrawal request, the client's account is temporarily frozen, and all gaming activity is suspended until the verification process has been finalized.

Handling CDD Non-Compliance

If a client fails to submit the required CDD documentation within 30 days of reaching the NAF 4,000 threshold, Pelican Entertainment B.V. initiates corrective action. The business relationship is terminated, and depending on the circumstances, the company takes the following steps:

If the situation gives rise to a reasonable suspicion of ML or TF, a Suspicious Transaction Report (STR) is submitted to the Financial Intelligence Unit (FIU).

In the absence of such suspicion, the remaining funds are returned to the original deposit source (e.g., the client's verified bank account or digital wallet).

If there are lingering concerns about possible financial crime, the company evaluates whether the funds should be frozen in accordance with its internal escalation procedures and regulatory requirements.

Measures to Prevent Tipping-Off

Pelican Entertainment B.V. is mindful of the risks associated with tipping off a client during account restriction or closure. In such cases, the company ensures that all actions are carried out discreetly and in accordance with legal obligations. Staff are guided by internal procedures designed to avoid breaching anti-tipping-off provisions while maintaining full regulatory compliance.

By ensuring that CDD measures are implemented swiftly and in alignment with financial activity thresholds, Pelican Entertainment B.V. strengthens its defenses against financial crime, upholds transparency, and safeguards the integrity of its gaming platform across all operational channels.

Ongoing Monitoring of Existing Clients

Pelican Entertainment B.V. applies Client Due Diligence (CDD) not only at the onboarding stage but also throughout the duration of the client relationship. The company is committed to maintaining a high standard of compliance by performing ongoing monitoring and routine reassessments, ensuring that all client activity remains consistent with prevailing Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) regulations.

Ongoing Assessment and Risk-Based Oversight

Client relationships are subject to continuous due diligence measures. This includes the regular monitoring of transactions and the reassessment of client risk profiles in light of new behaviors or patterns. Where necessary, the company re-evaluates previously collected data to ensure it remains accurate, complete, and relevant. Any deviation from expected conduct prompts further review and, where applicable, the application of enhanced scrutiny.

For clients who were previously onboarded with limited or incomplete CDD, Pelican Entertainment B.V. initiates retrospective due diligence procedures. These are prioritized based on risk, with high-risk clients undergoing immediate verification. Periodic updates are also conducted in accordance with both internal policies and regulatory guidance to ensure that CDD measures remain aligned with risk exposure and evolving compliance standards.

Reapplication of CDD Based on Risk Triggers

Pelican Entertainment B.V. applies full CDD measures to existing clients under specific conditions that indicate increased risk or regulatory necessity. These conditions include, but are not limited to:

A material change in the client's behavior or risk profile, such as sudden high-value transactions, relocation to a higher-risk jurisdiction, or being identified as a Politically Exposed Person (PEP).

Legislative or regulatory amendments that require updated or additional client verification.

The client engaging in one or more transactions totaling NAF 4,000 or more, which automatically triggers full identity verification and documentation review under the company's CDD policy.

Remediating Gaps in Historical CDD

In instances where clients were previously allowed to transact without complete CDD such as during legacy onboarding procedures or prior to the implementation of current regulatory standards Pelican Entertainment B.V. takes corrective action. High-risk clients are prioritized for immediate verification, while others are subject to a scheduled review based on the level of risk they present.

CDD is applied using a proportional and risk-sensitive approach, ensuring that resources are allocated where they are most needed and that lower-risk clients are still monitored effectively. Verification processes may include updated identity checks, refreshed PEP and sanctions screenings, and a reassessment of the client's source of funds and wealth.

By extending due diligence practices beyond initial onboarding and embedding them into the ongoing management of client relationships, Pelican Entertainment B.V. strengthens its regulatory compliance, reduces its exposure to financial crime, and upholds the integrity of its platform across all client segments.

Termination of Business Relationships

Pelican Entertainment B.V. maintains the right to terminate business relationships with clients who fail to comply with Client Due Diligence (CDD) requirements or who present heightened financial crime risks. This measure ensures the company's adherence to Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) regulations while preserving the security and integrity of its operations.

Business relationships are subject to termination when a client engages in suspicious or unexplained financial activities, fails to submit required CDD documentation within the prescribed timeframe, or is determined to pose a significant risk of involvement in money laundering or

terrorist financing. The decision to terminate a relationship is subject to formal internal review and must be approved by senior management.

Prior to termination, a final review of the client's account activity is conducted to identify any outstanding irregularities. If any transaction raises suspicion of ML, TF, or PF Pelican Entertainment B.V. submits a Suspicious Transaction Report (STR) to the Financial Intelligence Unit (FIU) without delay. All records associated with the terminated relationship are retained securely for a minimum of five years in accordance with regulatory requirements. This approach reinforces the company's commitment to proactive risk management and ensures regulatory compliance through the entire client lifecycle.

Where risk cannot be adequately mitigated such as uncooperative clients, unresolved discrepancies, or confirmed links to sanctioned entities Pelican Entertainment B.V. will terminate the business relationship and report such instances to the Financial Intelligence Unit (FIU)

Third-Party Reliance for Client Due Diligence

Pelican Entertainment B.V. may, under controlled circumstances, rely on qualified third parties to carry out specific components of the Client Due Diligence (CDD) process. Such reliance is implemented strictly within the boundaries of applicable AML/CTF/CPF laws and does not absolve the company of its legal responsibility to ensure full compliance. Pelican Entertainment B.V. remains ultimately accountable for the accuracy, completeness, and timeliness of all CDD-related activities performed on its behalf.

When relying on a third party, the company ensures that all relevant client identification and verification information is accessible without delay upon request. Third-party arrangements are governed by formal agreements that clearly outline data-sharing protocols, compliance obligations, and procedures for independent compliance audits. These agreements require the third party to be a regulated entity subject to robust AML/CFT supervision and to maintain an independent relationship with the client.

Importantly, Pelican Entertainment B.V. differentiates between third-party reliance and outsourcing. In a reliance scenario, the external party performs selected CDD tasks independently, while Pelican Entertainment B.V. retains full responsibility for assessing client risk, verifying Politically Exposed Person (PEP) status, and maintaining ongoing transaction monitoring. In an outsourcing arrangement, the third party operates under Pelican Entertainment B.V.'s direct oversight, following its internal policies and regulatory framework.

Before engaging with any third-party service provider, Pelican Entertainment B.V. conducts a comprehensive risk assessment of the provider's jurisdiction, evaluating its regulatory environment and compliance history. This is supported by intelligence from international

watchdogs and enforcement bodies. Regular assessments both quantitative and qualitative are performed to monitor the third party's performance and ensure the effectiveness of their procedures. These reviews verify that decisions regarding business relationships and risk classification remain under the exclusive control of Pelican Entertainment B.V.

Through structured oversight and stringent regulatory controls, Pelican Entertainment B.V. ensures that any third-party involvement in CDD processes contributes to a secure, transparent, and compliant operational environment.

10. Identifying Beneficial Ownership and Verifying the Control Structure

Pelican Entertainment B.V. undertakes all reasonable measures to identify, verify, and understand the Ultimate Beneficial Owners (UBOs) and the ownership and control structures of legal entity clients, in full compliance with AML Regulation III.2.2 and relevant international best practices.

This obligation extends beyond basic identification of beneficial owners and requires a full understanding of how ownership and control are exercised within the customer's structure, both at onboarding and throughout the course of the business relationship.

To meet this obligation, Pelican Entertainment B.V. applies the following measures:

- Identify and verify natural persons who ultimately own or control 25% or more of the equity, voting rights, or capital of a legal entity, whether directly or indirectly.
- Where no individual meets the ownership threshold, identify any persons who otherwise exercise effective control, such as through:
 - Voting arrangements, contractual relationships, or positions of influence (e.g., board control or management power).
 - Indirect control mechanisms, such as trusts, nominee arrangements, bearer shares, or layered ownership through multiple legal entities.
- Conduct multi-tiered analysis in cases where ownership is obscured through multiple corporate layers or complex holding structures, to trace and identify the natural person(s) exercising ultimate control.
- Obtain and review reliable documentation such as:
 - Shareholder registries, articles of incorporation, beneficial ownership registers.
 - Declarations from legal representatives clarifying control and ownership hierarchy.
 - Organizational charts and financial disclosures when necessary.
- Where no individual qualifies under the above, identify the most senior managing official as a fallback UBO, in accordance with the "last resort" principle under FATF and CGA guidance.
- Verify beneficial ownership and control details using independent and reliable sources, and ensure this information is:
 - Accurately recorded and readily available for competent authorities.
 - Regularly reviewed and updated, particularly when:
 - There is a change in ownership or control.
 - The customer's risk profile changes.
 - Trigger events occur (e.g., threshold transactions, suspicious activity).

Pelican Entertainment B.V. does not enter or continue business relationships with legal entities whose beneficial ownership or control structures are non-transparent, unverifiable, or otherwise obstructive to due diligence.

11. Monitoring of Transactions

Transaction monitoring within the betting and gambling sector plays a pivotal role in maintaining regulatory compliance and supporting anti-money laundering (AML) initiatives. With the industry's high transaction volumes and inherent risk exposure, regulators enforce strict oversight to prevent illicit activities such as money laundering, fraud, and terrorist financing. Pelican Entertainment B.V. is committed to addressing these challenges particularly those arising from the sheer speed and scale of transactions, as well as the growing use of cryptocurrencies and alternative digital payment methods, which add complexity to effective monitoring.

In essence, Curaçao's regulatory framework centers on identifying indicators of unusual or suspicious transactions that may warrant reporting to the Curaçao Financial Intelligence Unit (FIU Curaçao). As a result, a robust transaction monitoring system is essential for meeting the jurisdiction's licensing obligations.

Pelican Entertainment B.V.'s anti-fraud team manages a proprietary detection system that evaluates player activity through automated checks powered by tools such as WorldCheck, complemented by in-depth manual reviews conducted by trained analysts using multiple data sources. Any inconsistencies flagged at the first line of defence are escalated to the team lead and, when necessary, formally reported to the AML/CFT Officer via an internal Suspicious Activity Report (SAR).

The company's automated monitoring solution enables real-time oversight of all transactions, identifying suspicious behavior through predefined rules and risk thresholds. Leveraging machine learning and advanced data analytics, the anti-fraud team enhances detection accuracy while minimizing false positives. The system is specifically calibrated to spotlight high-risk activities including large deposits, repetitive transfers, and cross-border movements. Its parameters are continuously updated to reflect evolving threats, helping to identify and escalate suspicious behavior both internally and, where appropriate, to the relevant Financial Intelligence Units (FIUs).

System for Monitoring Transactions

Automated Monitoring System:

Pelican Entertainment B.V. employs advanced real-time monitoring technology that leverages algorithms and machine learning to detect unusual patterns or anomalies that may signal suspicious activity. These intelligent systems continuously analyze transactional behavior to identify potential risks with greater accuracy and speed.

Risk Assessment:

Each client and transaction is evaluated based on a comprehensive set of risk factors, including transaction size and frequency, geographic indicators, and behavioral trends. This risk-based approach ensures that high-risk activities receive enhanced scrutiny.

Alert Generation:

When the system identifies activity that deviates from established rules or thresholds such as

unusually large transactions or frequent deposits and withdrawals it automatically generates an alert. These alerts are then reviewed by the Compliance Officer for further investigation and action.

Common detection techniques include geolocation tracking, source-of-funds verification for high-value transactions, behavioral analytics to identify shifts in wagering patterns, and transaction velocity monitoring to detect rapid movement of funds or frequent high-value transfers within short timeframes.

Customer Due Diligence (CDD):

CDD measures are triggered in several scenarios, including:

Account creation

Doubts regarding the authenticity of client information or documents

Suspicious client profiles or transactional behavior

Unauthorized attempts to modify account details

Any transaction or linked transactions totaling 4,000 NAF or more

When a single transaction or a series of connected transactions exceeds the 4,000 NAF threshold (or equivalent), CDD is automatically applied. This includes deposits, withdrawals, wagers, and collection of winnings. Ongoing monitoring and periodic reviews of existing client records further support the CDD process.

Enhanced Monitoring for AML/CFT Prevention:

To combat money laundering, fraud, and terrorist financing, the proprietary anti-fraud platform tracks player IP addresses, ensuring access only from permitted jurisdictions. This control also assists in identifying attempts to create multiple accounts, as well as blocking blacklisted or self-excluded individuals.

The system further analyzes each player's transaction history, bet sizes, win-loss patterns, geolocation data, gambling behavior, and play duration. These insights help identify clients whose risk rating may be elevated due to behavioral or transactional red flags indicating possible AML/CFT concerns.

Failure to Complete CDD:

If a client is unable or unwilling to meet the CDD requirements, their account is immediately locked during the verification attempt. Ultimately, the business relationship is terminated in accordance with AML/CFT legislation, and any remaining funds are refunded using the original payment channel and account that were used to deposit the funds.

• **Politically- Exposed Persons (PEPs)**

Enhanced Due Diligence (EDD) is a crucial process in the online betting and gambling industries aimed at preventing money laundering, fraud, and other illicit activities. EDD refers to the additional measures taken by companies to thoroughly verify the identity and background of their clients, particularly those posing higher risks. High-risk clients in the online gambling and betting setting are those who have high transaction volumes, deposit or withdraw large amounts, exhibit unusual betting patterns or are Politically Exposed Persons (PEPs). A PEP is an individual who recently held

or is currently holding a prominent public position such as a head of state, member of the Parliament, government, directors of international organizations etc. Family members of PEPs and close associates are also considered PEPs, so their applications are also treated as high-risk by the Anti-Fraud team and relevant risk management procedures are activated when processing such requests through the senior management.

At Pelican Entertainment B.V. PEPs' cases are handled by the senior management team whose approval is necessary to transact with such individuals. Furthermore, an internal register of such cases is kept by the Compliance Officer.

- **Sanctions Management, FATF High-Risk List, License Restrictions**

Sanctions screening is the process of checking individuals, organizations, and transactions against various sanctions lists to prevent illegal activities and ensure compliance with international regulations. The purpose of sanctions screening is to comply with international, national, and regional sanctions regulations, prevent financial crimes such as money laundering and terrorism financing and to protect the reputation and integrity of the betting and gambling industry and Pelican Entertainment B.V. in particular. Whereas EDD focuses on enhanced verification of high-risk clients, sanctions screening specifically checks against sanctions lists to identify prohibited entities.

As a Curacao-based entity with an EU-based payment agent Pelican Entertainment B.V. complies with the key sanctions lists which are part of the international regulatory framework, including:

- United Nations Security Council (UNSC) Sanctions
- European Union (EU) Sanctions
- United States (OFAC) Sanctions: Office of Foreign
- Assets Control.
- UK Sanctions: HM Treasury Sanctions
- Other Jurisdictions: Local sanctions regulations.

If a match is identified on a sanctions list, Pelican Entertainment B.V. will immediately freeze associated assets without prior notice and notify the FIU in accordance with the Process for Freezing of Resources as published by the National Gazette (2016). Sanctions screening tools are updated in real-time, and a review of Curaçao Gaming Authority sanctions amendments is conducted at least monthly. All updates are reflected promptly in internal systems. Detailed Sanction Policy is described in Appendix III.

Update Mechanism and Frequency

Sanctions lists are updated at least daily and immediately upon publication of new updates by the competent authorities. Pelican Entertainment B.V. uses automated sanctions-screening tools that synchronize with official sources in real time to ensure that the most current sanctions information is applied. In addition, the Compliance Officer conducts a minimum monthly review of any amendments or circulars published by the Curaçao Gaming Authority or relevant government authorities to confirm alignment with local obligations.

Responsibilities

The Compliance Officer (or Sanctions Officer, where designated) is responsible for ensuring that sanctions lists are up to date, verifying tool synchronization, reviewing any alerts or potential matches, escalating confirmed matches, and ensuring adherence to regulatory requirements.

All sanctions-screening results, update logs, alerts, and match decisions are documented and retained for a minimum of five (5) years in accordance with applicable AML/CFT and sanctions regulations.

- **Suspicious Activity Reporting Guidelines**

The following transactions or intended transactions are deemed unusual:

Transactions which in connection with money laundering or terrorism financing are reported to the Police or to the Department of Justice.

Transactions by or on behalf of a natural or legal person, a group or an entity, who is named on a list, adopted by virtue of the Sanctions National Ordinance (N.G. 2014 no. 55);

Transactions in the amount of NAF. 5,000 or more, regardless of whether the transaction is made by check or other form of payment, or through electronic or other non- physical means.

Frequent high-value deposits followed by minimal play.

Structuring deposits to avoid reporting thresholds.

Use of third parties to obscure true ownership of funds.

This includes but is not limited to:

Accepting or releasing a deposit in the amount of NAF. 5,000 or more at the request of the client.

Deposits in the amount of NAF. 5,000 or more.

Withdrawal in the amount of NAF. 5,000 or more

According to article 1 of Norut, it is an internet gambling entity' s duty to report unusual transactions through the FIU Curacao's goAML portal which has been in use since January 1, 2021. Therefore, if the nominated officer determines that the internally reported suspicious activity should be disclosed to the regulatory authorities, he does so via the portal to comply with the Company's AML/CFT reporting protocol and obligations. In the meantime, the business relationship with the suspected client is to be paused or terminated, depending on the circumstances.

Prohibition of Disclosure

To maintain the integrity of the reporting process and comply with legal obligations, our policy strictly prohibits the disclosure of any information related to suspicious activity reports (SARs) to the subjects of such reports or unauthorized parties. This prohibition is crucial to prevent potential interference with ongoing investigations or legal proceedings. Employees are required to handle all related communications discreetly and are only permitted to discuss SARs with the Compliance Officer or other authorized personnel. Any breach of this confidentiality requirement will be treated

as a serious violation of our ML/FT/FP policy and may result in disciplinary action. This ensures that the reporting process remains confidential and effective in addressing potential threats

Suspicious activity may include using several anonymous payment methods

i.e. prepaid cards; location of the payment method does not correspond to the geolocation of the client; depositing a large sum and withdrawing it after no gaming or little gaming activity; a withdrawal request to a third-party payment method.

Suspicious activity may include using an intermediary for document-related requests; source of wealth does not match the reported financial data; frequent changes of ownership in a short time; lack of willingness to provide due diligence documentation.

Pelican Entertainment B.V. keeps detailed records of all transactions and activities that seem suspicious, including dates, amounts, methods, and any other relevant details. As regards clients, the anti-fraud and AML teams document all available information about the individuals or entities involved, including names, addresses, account numbers, and identification.

Detecting Unusual Transactions

Pelican Entertainment B.V. defines an unusual transaction as any financial activity that deviates materially from a client's established behavior or declared financial profile. These may include large or unexpected money movements, transactions involving unknown or unverified third parties, or financial activity lacking a clear legal or economic purpose.

The company relies on advanced transaction monitoring systems to detect such anomalies. When flagged, these transactions are forwarded to the Compliance Officer for deeper review. Staff members are trained to recognize behavioral and transactional red flags and to act promptly in escalating concerns.

The following categories of transactions are considered particularly noteworthy and may trigger further examination or reporting:

Previously Reported Activities: Transactions already identified and forwarded to judicial or law enforcement agencies such as the police or public prosecutor for potential links to ML or TF are automatically categorized as unusual.

Dealings with Sanctioned Persons or Entities: Any transaction involving a party listed under the Sanctions National Ordinance (N.G. 2014 no. 55), or other relevant sanction regimes, is flagged and treated as unusual.

High-Value Transactions: Transactions equal to or exceeding NAF 5,000 regardless of the method of payment are subject to scrutiny. This includes:

Deposits or withdrawals at or above the threshold.

Purchases of gaming tokens, digital credits, or chips meeting or exceeding the limit.

Redemptions or payouts of winnings at or above the specified amount.

The threshold also applies to a series of transactions that cumulatively total NAF 5,000 or more within a single gaming day. Such cumulative activity is evaluated in aggregate when determining whether reporting is necessary.

In cases where there is a reasonable basis to suspect that a transaction is connected to ML, TF, or PF whether due to the nature of the transaction, the behavior of the client, or other risk indicators it must be treated as suspicious and subject to internal escalation procedures.

Timely Reporting to the FIU

Once a transaction is determined to be unusual or suspicious, Pelican Entertainment B.V. is obligated to file a report with the Financial Intelligence Unit (FIU) without delay, in accordance with AML Regulation IV.1. This requirement applies whether the transaction has been completed or merely attempted. The Compliance Officer is responsible for submitting the Unusual Transaction Report (UTR) immediately after the suspicion is confirmed, without waiting for additional approvals or administrative processes.

Confidentiality in Reporting

Maintaining strict confidentiality around Suspicious Activity Reports (SARs) is fundamental to preserving the effectiveness of the company's compliance regime and fulfilling its legal obligations. Employees are strictly prohibited from disclosing any details of a SAR to the person under review or to any unauthorized third party. Breaches of this confidentiality can undermine investigations, result in regulatory violations, and constitute a tipping-off offence under applicable legislation.

Only authorized personnel such as the Compliance Officer and designated members of the compliance team may handle SAR-related information. All such communications must be treated with the highest level of discretion. Pelican Entertainment B.V. provides regular training to ensure staff understand the importance of maintaining confidentiality in all aspects of the reporting process.

Violations of this confidentiality policy are treated as serious compliance breaches and may lead to disciplinary action, including termination of employment. These protocols are critical to maintaining the integrity of the reporting framework and the company's ability to respond effectively to financial crime risks.

By fostering a culture of awareness, discretion, and accountability, Pelican Entertainment B.V. strengthens its ability to identify suspicious behavior, uphold its obligations under AML/CTF/CPF regulations, and support broader efforts to prevent financial crimes across the iGaming sector.

12. Reporting Unusual Transactions “Without Delay”

In accordance with the National Ordinance on the Reporting of Unusual Transactions (NORUT), the Company is legally required to report all Unusual Transactions (UTRs) to FIU Curacao “without delay” as per requirement in Art. 30(2) of the 2025 Regulations and Art. 8 NORUT.

To operationalize this legal requirement, the Company establishes the following internal reporting timelines:

- Immediate escalation from staff to Compliance Officer:
- Internal review and validation by Compliance Officer:
- Submission to FIU Curaçao: always without delay, in line with NORUT requirements.

Under no circumstances may the client be informed that an Unusual Transaction Report (UTR) has been filed (“tipping-off”).

Deposits or withdrawals at or above the threshold.

Purchases of gaming tokens, digital credits exceeding the limit.

Redemptions or payouts of winnings at or above the specified amount.

The threshold also applies to a series of transactions that cumulatively total NAF 5,000 or more within a single gaming day. Such cumulative activity is evaluated in aggregate when determining whether reporting is necessary.

In cases where there is a reasonable basis to suspect that a transaction is connected to ML, TF, or PF whether due to the nature of the transaction, the behavior of the client, or other risk indicators it must be treated as suspicious and subject to internal escalation procedures.

Timely Reporting to the FIU

Once a transaction is determined to be unusual or suspicious, **Pelican Entertainment B.V.** is obligated to file a report with the Financial Intelligence Unit (FIU) without delay, in accordance with AML Regulation IV.1 and reporting requirement under Article 30(2) of the January 2025 AML/CFT/CPF Regulations, reinforced by Article 8 NORUT, ensuring that all internal alerts, investigations, and external filings occur promptly and in accordance with the statutory timeline. This requirement applies whether the transaction has been completed or merely attempted. The Compliance Officer is responsible for submitting the Unusual Transaction Report (UTR) immediately after the suspicion is confirmed, without waiting for additional approvals or administrative processes.

Confidentiality in Reporting

Maintaining strict confidentiality around Suspicious Activity Reports (SARs) is fundamental to preserving the effectiveness of the company’s compliance regime and fulfilling its legal obligations. Employees are strictly prohibited from disclosing any details of a SAR to the person under review or to any unauthorized third party. Breaches of this confidentiality can undermine investigations, result in regulatory violations, and constitute a tipping-off offence under applicable legislation.

Only authorized personnel such as the Compliance Officer and designated members of the compliance team may handle SAR-related information. All such communications must be treated with the highest level of discretion. **Pelican Entertainment B.V.** provides regular training to ensure staff understand the importance of maintaining confidentiality in all aspects of the reporting process.

Violations of this confidentiality policy are treated as serious compliance breaches and may lead to disciplinary action, including termination of employment. These protocols are critical to maintaining

the integrity of the reporting framework and the company's ability to respond effectively to financial crime risks.

By fostering a culture of awareness, discretion, and accountability, **Pelican Entertainment B.V.** strengthens its ability to identify suspicious behavior, uphold its obligations under AML/CTF/CPF regulations, and support broader efforts to prevent financial crimes across the iGaming sector.

13. Compliance Officer

Compliance Officer, or Money Laundering Reporting Officer is a designated individual who oversees compliance with AML regulations at Pelican Entertainment B.V. It is a crucial role which encompasses being authorized to communicate with the relevant authorities in Curacao as well as supervise a team of AML compliance officers and their day-to-day operations, including maintaining robust age verification protocols, promoting responsible gambling practices, preventing gambling-related addiction, promoting self-exclusion tools.

The Compliance Officer of Pelican Entertainment B.V. operates with full independence and is granted the necessary authority to perform all duties related to the Anti-Money Laundering, Counter-Terrorism Financing, and Counter-Proliferation Financing (AML/CTF/CPF) compliance framework. The Compliance Officer has unrestricted and direct access to all relevant customer information, transaction data, internal systems, and personnel, as required to fulfill their compliance obligations effectively. To preserve independence and avoid conflicts of interest, the Compliance Officer reports directly to the Board of Directors and is not involved in any operational or commercial functions of the company that could compromise objectivity. The Board ensures the Compliance Officer is adequately resourced, empowered, and supported in executing the AML/CTF/CPF program in accordance with Regulation V.3 of the CGA AML Guidelines. This structure safeguards the autonomy of the compliance function and ensures timely escalation of significant risks or breaches to the highest level of governance.

The Compliance Officer is also responsible for disclosing suspicious activity, including suspicious transactions, to the FIU in Curacao. Internally, the AML/CFT Officer is requested to prepare quarterly AML reports for the Board of Directors to keep the Board members informed of any recommended changes that may be required to manage the AML/CFT compliance program.

The Compliance Officer is tasked with several critical functions to ensure the effectiveness of our AML program. These primary duties include:

- **Policy Implementation:** Overseeing the execution of AML policies and procedures to ensure alignment with current regulations.
- **Central Point of Contact:** Serving as the main contact for all AML-related issues.
- **Policy Review:** Regularly reviewing and updating AML policies to address evolving regulatory standards and emerging risks.
- **Training Oversight:** Managing the AML training program to ensure employees are adequately informed about AML requirements and their roles in maintaining compliance.
- The Compliance Officer is entrusted with several essential responsibilities:

- **Transaction Monitoring and Reporting:** Continuously analysing transactions and client activities to identify suspicious behaviour. They are responsible for filing Suspicious Activity Reports (SARs) with the Financial Intelligence Unit (FIU) when necessary and maintaining accurate records of these reports.
- **Policy Development and Updates:** Crafting and revising AML policies and procedures to adhere to the latest Curaçao gaming regulations and international best practices. This includes adapting the AML framework to address new risks and regulatory changes.
- **Employee Training and Awareness:** Ensuring that all staff receive comprehensive AML training and understand their responsibilities in detecting and reporting suspicious activities. The Compliance Officer must regularly update training materials to reflect legislative or policy changes.
- **Regulatory Liaison:** Acting as the primary contact with regulatory bodies, law enforcement, and other relevant authorities on AML matters. This includes responding to information requests and participating in regulatory inspections or audits.
- **Compliance Audits:** Conducting regular reviews and audits of the AML program to evaluate its effectiveness and compliance with legal requirements. The Compliance Officer is responsible for addressing any identified issues and implementing necessary corrective measures.
- **Record-Keeping:** Maintaining detailed records of all AML-related activities, including SARs, internal reports, training sessions, and policy updates. These records must comply with legal requirements and be readily available for regulatory review.
- Through the execution of these functions and responsibilities, the Compliance Officer plays a vital role in safeguarding the organization against money laundering and terrorist financing risks, ensuring rigorous compliance with Curaçao's AML regulations.

14. Senior Management Responsibility

The Company's senior management holds a central role in identifying, assessing, and managing the inherent risks associated with money laundering, terrorist financing, and proliferation financing (ML/FT/FP). The Board of Directors requires that a designated AML/CFT Officer provide regular updates on any material deviations within the control environment. This officer is also responsible for submitting an annual report evaluating the effectiveness of the Company's systems and controls in mitigating ML/FT/FP risks.

To maintain a strong compliance posture, senior management ensures that all relevant policies and procedures undergo comprehensive review at least once per year. These reviews are informed by monthly risk assessments, enabling the timely detection of potential control gaps or weaknesses in risk mitigation strategies. Where deficiencies are identified, the AML/CFT Officer is authorized to recommend corrective measures for Board approval, reinforcing the Company's commitment to a dynamic and responsive risk management framework.

In alignment with international best practices, senior management also oversees the implementation of comprehensive training programs for employees. These programs are tailored to promote a deep understanding of ML/FT/FP threats, ensuring that all staff particularly those in

sensitive or high-risk roles are equipped to recognize and respond to suspicious activities appropriately.

Moreover, senior management is responsible for ensuring the Company's internal control structure is both effective and resilient. This includes enforcing clear segregation of duties, well-defined authorization protocols, ongoing monitoring mechanisms, and thorough documentation standards. To support continuous improvement, the Company conducts regular independent audits and evaluations of its ML/FT/FP program to objectively assess performance, identify enhancement opportunities, and uphold full compliance with applicable regulatory obligations.

GCB Supervision and Enforcement

The Company operates under the direct supervision of the Curaçao Gaming Authority (GCB), as established in Article 4(1) LOK, which serves as the competent AML/CFT/CPF supervisor for the gaming sector. which designates the GCB as the competent authority responsible for AML/CFT/CPF supervision of licensed gaming operators.

Pursuant to its statutory mandate under Articles 5–9 LOK, the GCB is empowered to:

- Conduct on-site and off-site AML/CFT/CPF examinations (Art. 7 LOK);
- Request and obtain unrestricted access to documents, systems, data, and personnel (Art. 8 LOK);
- Assess the implementation of operator obligations under the Regulations for the Combatting of Money Laundering, Terrorist Financing, and Proliferation Financing (effective 1 January 2025), issued under Art. 11 LOK;
- Issue binding directives, mandatory remediation instructions, or improvement plans (Art. 9(1)(b) LOK);
- Impose administrative sanctions, including fines, conditional measures, license restrictions, suspension, or revocation (Art. 15–18 LOK).

The Company acknowledges that the January 2025 AML/CFT/CPF Regulations have binding legal effect under Art. 11 LOK, and non-compliance constitutes a regulatory breach subject to GCB enforcement actions under Art. 15-18 LOK.

15. Employee Training and Screening Program

Employees in the betting and gambling industries are on the front lines of AML compliance. Pelican Entertainment B.V. conducts its operations with a high standard of ethics, ensuring full compliance with laws and regulations governing financial transactions. The company has implemented policies and procedures for screening employees for criminal records, as part of its ongoing commitment to integrity.

To ensure the integrity and competence of personnel engaged in activities relevant to anti-money laundering (AML) and counter-terrorist financing (CTF) obligations, the Company maintains a structured Employee Screening Program in accordance with CGA AML Regulation V.4. Please see Appendix II.

Pelican Entertainment B.V.'s employees play a crucial role in Anti-Money Laundering (AML) compliance within the betting and gambling industries. Their actions and vigilance are essential in preventing these sectors from being exploited for money laundering and other illicit activities. They

are made aware of the fact that failing to report potential breaches of AML Policies may lead to administrative and criminal charges.

The Company's employees, especially those in client-facing roles or positions that involve handling financial transactions, must have a thorough understanding of the company's AML policies and procedures. This includes knowing the types of transactions that should be considered suspicious, the process for reporting such transactions, and the importance of maintaining client confidentiality.

A key part of an employee's role in AML compliance is to be vigilant and identify any activities that seem unusual or do not fit with the normal behaviour of a client. This could include large and inconsistent bets, frequent changes in betting patterns, or transactions that seem to have no apparent purpose other than to move money through the system.

Once an employee identifies a potentially suspicious transaction, they must report it through the appropriate channels to the Compliance Officer. The reporting protocol involves filling out a Suspicious Activity Report (SAR) and using the company's internal reporting system. Employees are trained on how to report suspicions and the importance of doing so promptly on an annual basis or more frequently in line with the needs of a particular department.

Employees involved in client onboarding or account management are responsible for conducting due diligence checks on clients. This includes verifying their identity, understanding the source of their funds, and ensuring that they are not listed on any sanctions or watch lists. Employees are trained on how to conduct such checks diligently and escalate any concerns where necessary.

Employees involved in AML compliance at Pelican Entertainment B.V. understand the importance of maintaining the confidentiality of their reports and any information related to suspicious activities. They are made aware of data protection laws and ensure that client information is handled in compliance with these regulations.

Pelican Entertainment B.V. upholds the highest standards of integrity and professionalism among its personnel, recognizing employees as critical to the company's Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) compliance framework. In line with Regulation V.4 of the CGA AML Guidelines, the company maintains a formal Employee Screening Program, applied both prior to employment and on an ongoing basis thereafter.

15.1 . Pre-Employment Screening

Before onboarding any new employee, especially those in sensitive, client-facing, or compliance-related roles, the company conducts thorough background checks, including:

- Verification of identity and right to work using government-issued documentation.
- Criminal background checks to detect any prior financial or integrity-related offenses.
- Employment and reference verification to confirm qualifications and experience.
- Sanctions and PEP screening, using independent screening tools and global watchlists.

Candidates failing to meet the company's integrity or risk criteria are not employed.

15.2 Ongoing Employee Screening

Pelican Entertainment B.V. continues to assess employee suitability after hiring through:

- Annual rescreening of employees in AML/CTF-sensitive roles.
- Event-driven screening, such as when suspicious activity, misconduct, or role changes occur.
- Monitoring for changes in sanctions exposure, PEP status, or relevant legal/regulatory risks.

All employee screening records are retained securely and confidentially, in compliance with data protection laws, for a minimum of five (5) years.

15.3 Training and Awareness

Employees, particularly those involved in onboarding, account management, or transaction processing, receive annual AML/CTF training tailored to their roles. This training ensures staff understand:

- The company's AML/CTF/CPF obligations.
- How to identify unusual behavior, such as:
 - Large or inconsistent bets.
 - Suspicious patterns of deposits/withdrawals.
 - Anonymous or third-party payments.
- How and when to file a Suspicious Activity Report (SAR).
- The importance of confidentiality and client data protection.

Employees are made aware that failure to comply with AML/CTF obligations may lead to disciplinary, administrative, or criminal consequences.

16. Record- Keeping

Pelican Entertainment B.V. is subject to The Company complies with all the relevant legislation as regards having an audit trail in cases where it is asked to assist in the investigations by law enforcement agencies. Generated records are retained in electronic form for a period of 5 years in accordance with the data protection regulations from the date of the establishment of a business, commercial or a professional relationship with an employee, a client or a business partner.

To adhere to stringent record-keeping standards, our company implements robust procedures for managing documentation associated with AML/CTF/CPF. We maintain comprehensive records, which include client identification information, transaction details, suspicious activity reports (SARs), training logs, and audit records, all preserved for a minimum of five years.

- The company securely maintains detailed records, including:
- Client identification information.
- Transaction histories.

- Suspicious activity reports (SARs).
- Staff training logs.
- Audit records.

We ensure the security of these records through advanced encryption techniques and strict access controls to prevent unauthorized access. Regular audits are conducted to verify the integrity of the data and safeguard against potential breaches.

A systematic approach is adopted for organizing records, allowing for efficient retrieval by authorized personnel and regulatory bodies. We conduct continuous internal monitoring and periodic audits to ensure compliance with established protocols.

By effectively managing our records, the company not only meets regulatory requirements but also facilitates auditing processes and contributes to the overall integrity of the gaming industry.

17. AML Compliance Audit

In adherence to the new Curacao gaming legislation and Section V.5 of the Curaçao Gaming Authority's AML Guidelines, the company is required to undergo an independent Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF) and Counter-Proliferation Financing (CPF) audit. This chapter outlines the framework for conducting such audits, the roles of independent audit functions, and the examination process by the Gaming Authority.

To this end, the Company conducts periodic AML compliance audits, at least annually and additionally in the event of significant regulatory changes, operational developments, or material compliance breaches. These audits are carried out by qualified internal or external parties who are independent from daily compliance operations and who possess the requisite expertise in financial crime risk management.

The audit scope includes, but is not limited to:

- Evaluation of Policies and Procedures – Reviewing whether the AML/CTF/CPF framework is up to date, aligned with legal standards, and effectively applied across departments.
- Effectiveness of Risk-Based Approach – Testing the design and implementation of Business Risk Assessments (BRA), Customer Risk Assessments (CRA), and other relevant methodologies.
- Transaction Monitoring and SAR/STR Filing – Assessing the adequacy of transaction surveillance tools and the timeliness, quality, and completeness of suspicious activity reporting.
- CDD and KYC/KYB Compliance – Sampling client files to verify that due diligence procedures, beneficial ownership checks, and document retention policies are implemented correctly.
- Sanctions Screening Controls – Verifying the application and currency of screening mechanisms against relevant international and domestic sanctions lists.

- Employee Screening and Training – Assessing adherence to employee screening requirements and the effectiveness of ongoing AML training programs.
- Technology Risk Controls – Reviewing systems supporting AML compliance, including data integrity, automated risk scoring, and access rights.

The outcomes of the internal audits are formally documented in comprehensive reports, which are submitted directly to senior management and the Board of Directors, in accordance with CGA AML Regulation Section V.7. These reports identify any deficiencies or areas for improvement and include clear recommendations and timelines for remediation.

Furthermore, audit findings that reveal material weaknesses, breaches, or risks to AML/CTF/CPF compliance are escalated immediately to the Compliance Officer and the Board, with follow-up audits conducted to verify implementation of corrective actions.

Pelican Entertainment B.V. maintains an audit trail and full documentation of all internal audit activities for a minimum of five (5) years and makes such records immediately available to the Curaçao Gaming Authority (CGA) upon request. The Company is committed to transparency, accountability, and continuous improvement in its AML/CTF/CPF compliance framework.

18. Regulatory Access and Cooperation

The Company confirms that it is subject to the supervisory and enforcement powers granted to the Curaçao Gaming Control Authority (CGA) under the National Ordinance on the Supervision and Regulation of the Gaming Sector (LOK). Under Article 9 LOK, all supervisory instructions, directives, and remedial measures issued by the GCB are legally binding and enforceable.

The Company further acknowledges that the development and implementation of its internal systems, controls, monitoring mechanisms, and reporting processes are designed to fully comply with:

- Part II (Articles 3–13) of the January 2025 AML/CFT/CPF Regulations (governance, risk management, internal controls);
- Part III (Articles 14–27) (CDD, EDD, ongoing monitoring);
- Part IV (Articles 28–35) (recordkeeping, reporting, internal audit, employee training).

The Company commits to full cooperation with the GCB during all supervisory examinations, information requests, and enforcement processes pursuant to Articles 5–9 LOK.

Pelican Entertainment B.V. fully acknowledges the supervisory and enforcement authority of the Curaçao Gaming Control Authority (CGA) as prescribed in Section V.6 of the GCB AML Guidelines and commits to complete, proactive cooperation with all regulatory examinations and oversight activities. To this end, the company grants the GCB and any other legally empowered authority unrestricted, immediate, and comprehensive access to all data, systems, records, and personnel necessary for the assessment of its Anti-Money Laundering, Counter-Terrorism Financing, and Counter-Proliferation Financing (AML/CTF/CPF) framework.

This includes, but is not limited to:

- Customer due diligence records
- Transaction histories and monitoring data
- Internal risk assessments
- Policies and procedures
- Communication logs and training materials
- Audit trails, reports, and logs
- Compliance-related systems and platforms

Access shall be granted for both on-site and remote inspections, including the right to request supplementary documentation, system walkthroughs, and clarifications. Pelican Entertainment B.V. ensures that all required information is readily retrievable, promptly provided upon request, and securely maintained for a minimum of five (5) years, or longer where legally mandated. Furthermore, the company commits to full cooperation with any post-inspection findings, including corrective action plans and remedial steps as directed by the GCB.

19. Internal Audit and Reporting

Pelican Entertainment B.V. shall establish and maintain an independent internal audit function for the purpose of evaluating the effectiveness, adequacy, and operational integrity of its Anti-Money Laundering, Counter-Terrorist Financing, and Counter-Proliferation Financing (AML/CTF/CPF) framework. Internal AML audits shall be conducted at least annually, or at such greater frequency as may be necessitated by the Company's risk exposure, regulatory developments, or material changes to business operations. Audits shall be performed by the Internal Audit team, or by an independent third-party auditor where required to ensure full independence, objectivity, and professional competence.

The scope of each internal audit shall include, but shall not be limited to: the review and testing of AML/CTF/CPF policies and procedures; assessment of the effectiveness of transaction monitoring systems and sanctions-screening controls; verification of the adequacy and accuracy of Suspicious Activity Report (SAR) filings; evaluation of customer due diligence and enhanced due diligence practices; examination of training programs and training effectiveness; and testing of governance, oversight, and record-keeping arrangements. The audit shall also assess whether the Company's systems and controls remain proportionate to its risk profile and compliant with statutory and regulatory obligations.

Upon completion of each audit, a formal Internal Audit Report shall be issued, setting out the audit methodology, findings, deficiencies identified, and recommended remedial actions. Such reports shall be submitted without delay to Senior Management and the Board of Directors, or any duly authorized committee with oversight responsibilities. Senior Management shall ensure that all identified deficiencies are addressed and rectified within defined and documented timeframes, and that implementation of corrective actions is monitored to completion.

All internal audit reports, supporting documentation, working papers, and remedial action logs shall be maintained in a secure and tamper-proof manner and retained for a minimum period of five (5) years, or longer where required by law or regulation. The internal audit function shall have unrestricted, unimpeded access to all systems, personnel, records, and information necessary to discharge its duties effectively and in full compliance with applicable regulatory expectations.

20. Regulatory Access and Legal Force

The Company confirms that it is subject to the supervisory and enforcement powers granted to the Curaçao Gaming Authority (CGA) under the National Ordinance on the Supervision and Regulation of the Gaming Sector (LOK). Under Article 9 LOK, all supervisory instructions, directives, and remedial measures issued by the GCB are legally binding and enforceable.

The Company further acknowledges that the development and implementation of its internal systems, controls, monitoring mechanisms, and reporting processes are designed to fully comply with:

- Part II (Articles 3–13) of the January 2025 AML/CFT/CPF Regulations (governance, risk management, internal controls);
- Part III (Articles 14–27) (CDD, EDD, ongoing monitoring);
- Part IV (Articles 28–35) (recordkeeping, reporting, internal audit, employee training).

The Company commits to full cooperation with the GCB during all supervisory examinations, information requests, and enforcement processes pursuant to Articles 5–9 LOK.

Pelican Entertainment B.V. fully acknowledges the supervisory and enforcement authority of the Curaçao Gaming Authority (CGA) as prescribed in Section V.6 of the GCB AML Guidelines and commits to complete, proactive cooperation with all regulatory examinations and oversight activities. To this end, the company grants the GCB and any other legally empowered authority unrestricted, immediate, and comprehensive access to all data, systems, records, and personnel necessary for the assessment of its Anti-Money Laundering, Counter-Terrorism Financing, and Counter-Proliferation Financing (AML/CTF/CPF) framework.

This includes, but is not limited to:

- Customer due diligence records
- Transaction histories and monitoring data
- Internal risk assessments
- Policies and procedures
- Communication logs and training materials
- Audit trails, reports, and logs
- Compliance-related systems and platforms

Access shall be granted for both on-site and remote inspections, including the right to request supplementary documentation, system walkthroughs, and clarifications. Pelican Entertainment B.V. ensures that all required information is readily retrievable, promptly provided upon request, and securely maintained for a minimum of five (5) years, or longer where legally mandated. Furthermore, the company commits to full cooperation with any post-inspection findings, including corrective action plans and remedial steps as directed by the GCB.

Binding Legal Effect

The Company acknowledges that as of January 2025, all provisions of the AML/CFT/CPF Regulations carry binding legal effect pursuant to the National Ordinance on the Supervision and Regulation of the Gaming Sector (LOK) and related AML/CFT legislation including NOIS, NORUT,

NOPML, and the Sanctions National Ordinance (SNO). Failure to comply may result in administrative sanctions, mandatory remediation, license restriction, suspension, or revocation.

The Company ensures that all employees and management are aware of the binding nature of these Regulations and that all internal controls are designed to fully comply with

21. Risk Factors

Customer Risk and Risk-Based Assessments

Customer risk represents the likelihood of exposure to money laundering (ML) and terrorist financing (TF) stemming from interactions with specific individuals. As part of its risk-based compliance model, **Company** evaluates customer profiles based on identity, financial behavior, source of wealth, and transaction history to identify and manage potential vulnerabilities.

Certain customer segments are inherently riskier. These include individuals with multiple or unverifiable income sources, those with inconsistent financial patterns, and **Politically Exposed Persons (PEPs)**—who, due to their public positions and access to state funds, are subject to elevated scrutiny for corruption and abuse of power.

Additional high-risk profiles may include:

- **High spenders** whose financial activity exceeds their declared income;
- **Disproportionate spenders** engaging in transactions beyond reasonable financial means;
- **Customers using multiple accounts**, who may attempt to disguise betting behavior or evade detection.

To address these risks, **Company** has established transaction thresholds aligned with expected customer behavior. While low-risk individuals typically have a single, verifiable income source, higher-risk customers are subject to enhanced due diligence (EDD) and ongoing transaction monitoring.

Product, Service, and Transaction Risks

Certain gaming offerings and transaction types present a greater risk of exploitation for ML/TF. Criminal organizations may exploit vulnerabilities within gaming ecosystems to conceal the origin of illicit funds.

Common risks include:

- **Use of criminal proceeds** from activities like fraud, trafficking, or theft deposited into gaming accounts;
- **Anonymous payment methods**, such as prepaid cards or cryptocurrencies, which offer limited traceability;
- **Gaming accounts used solely for deposits/withdrawals**, without genuine gaming activity;
- **Peer-to-peer transfers**, enabling covert fund movement between users;
- **Use of third-party financial tools**, such as bank accounts or cards not registered to the customer;

- **Cross-platform fund transfers**, which make tracking more complex;
- **Multi-operator gaming networks**, allowing users to circumvent controls through layered accounts.

To mitigate these risks, **Company** conducts ongoing transaction monitoring, applies EDD measures where needed, and ensures strict compliance with global AML/CTF/CPF standards.

Geographical Risk

Geographical risk refers to threats associated with the locations of customers or the origin of their funds, particularly from jurisdictions with poor AML/CTF oversight, high corruption levels, or active sanctions.

High-risk regions are monitored using trusted sources such as:

- **FATF high-risk and monitored jurisdictions;**
- **CFATF regional advisories;**
- **U.S. Department of State INCSR reports;**
- **EU lists of high-risk third countries;**
- **OFAC sanctions and enforcement actions;**
- **Transparency International's Corruption Perceptions Index (CPI).**

Company utilizes a country classification model to distinguish high- and low-risk jurisdictions. Customers from high-risk regions are subject to EDD, stricter onboarding processes, and heightened transaction monitoring. Transactions involving sanctioned countries are blocked, and monitoring protocols are regularly updated to reflect the latest geopolitical developments and compliance risks.

Distribution Channel Risks and Controls

The manner in which **Company** delivers its services can also pose financial crime risks—especially through channels that allow for anonymity or reduced oversight.

To counter these risks, the company enforces:

- **Stringent verification for non-face-to-face transactions;**
- **Biometric and multi-factor authentication technologies;**
- **Advanced identity verification systems** to ensure genuine user interaction.

These efforts help prevent fraud, detect high-risk behaviors early, and support compliance with international regulatory standards, ensuring that all customer engagement channels remain secure and transparent.

Technological Developments Risk Assessment

As the iGaming sector rapidly evolves through technological innovation, **Company** is committed to ensuring that new digital capabilities do not create opportunities for financial crime. The company has embedded a proactive **technological risk assessment process** into its compliance framework to identify and mitigate risks linked to new products, services, and operational technologies.

Technology-Driven Risk Identification

Company conducts comprehensive evaluations whenever:

- A **new product** or **feature** is launched;
- A **business process** is updated or automated;
- A new **payment method** or **digital platform** is introduced;
- Advanced technologies—such as **blockchain**, **AI**, or **automated services**—are adopted.

Each innovation undergoes a full compliance risk assessment to determine whether it could be misused for illicit purposes. Findings are documented, and control measures are applied in line with both Curaçao's legal requirements and international AML/CTF expectations.

Implementation of Technological Safeguards

When potential risks are identified, **Company** takes immediate action through:

- **Enhanced security infrastructure**, including biometric verification, encryption, and AI-powered fraud detection;
- **Upgraded transaction monitoring systems** capable of identifying suspicious patterns tied to new technologies;
- **Policy updates** to reflect emerging digital risks and evolving criminal methodologies.

This ensures the company remains compliant, secure, and adaptive to changes in the tech landscape.

By continuously assessing technological risk, refining controls, and adapting policies, **Company** preserves the integrity of its operations while maintaining full compliance with AML/CTF/CPF obligations. This forward-looking approach ensures that innovation and security evolve together, enabling the company to remain both competitive and compliant in a rapidly transforming industry.

22. Due Diligence

Company (Reg. Number: 141651) is firmly committed to regulatory compliance and the prevention of anonymous or fraudulent accounts. As part of its Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) framework, the company enforces strict identity verification procedures to ensure all business relationships with players are legitimate.

Through the implementation of comprehensive Customer Due Diligence (CDD) protocols, **Company** is equipped to identify and mitigate risks associated with financial crime, including money laundering, terrorism financing, and proliferation financing. All suspicious activity uncovered during the due diligence process is reported to the Financial Intelligence Unit (FIU), with serious cases escalated to the Public Prosecutor's Office when appropriate. These proactive measures reflect Company's commitment to regulatory adherence and responsible gaming.

Comprehensive Customer Due Diligence Measures and Client Acceptance Policy

Player Identification and Verification

As part of its CDD program, **Company** applies a rigorous identity verification process that includes:

- Validation of identity through trusted, independent sources (e.g., government-issued ID).
- Identification of Ultimate Beneficial Owners (UBOs) for corporate entities.
- Understanding the nature and purpose of the business relationship.
- Continuous monitoring to ensure financial activity aligns with customer risk profiles and declared source of funds.

Confidential Reporting Procedures

To prevent tipping off customers, Company employees are strictly prohibited from disclosing when a Suspicious Activity Report (SAR) has been filed with the FIU. If standard CDD procedures might reveal that an investigation is underway, the company may bypass certain steps and report the activity immediately.

Player Identity Verification Process

Required Information

Players must provide:

- Full legal name
- Date and place of birth
- Residential address
- Nationality
- Official ID number (passport, ID card, or driver's license)

For low-risk individuals, this basic data may suffice. High-risk individuals are subject to additional verification measures.

Risk Assessment and Validation

Upon registration, each player undergoes a risk assessment, updated continuously as new data becomes available. Verification includes:

- Review of photo ID
- Address confirmation through recent documents
- Biometric checks and database cross-matching
- IP tracking and source of funds analysis

If initial data is insufficient, Company may require:

- A live selfie with identification
- Verification of the first deposit from a regulated institution

Understanding the Business Relationship

Company seeks to understand the nature of each customer relationship. While the primary purpose is clear—online gaming—the company gathers data to detect unusual or suspicious activity.

For high-risk customers, **Enhanced Due Diligence (EDD)** includes:

- Documentation of source of wealth
- Analysis of financial and gaming behavior
- Cross-checks against third-party databases

Low- and medium-risk customers may provide:

- A basic employment or income declaration
- Additional information only if anomalies are detected

This tiered approach ensures proportional due diligence while meeting compliance obligations.

Ongoing Monitoring and Compliance Oversight

Company continuously monitors players and their transactions as part of its AML/CTF/CPF program.

Key actions include:

- Regular updates to player information, especially for high-risk accounts
- Transaction monitoring to detect suspicious patterns
- EDD applied to transactions equal to or exceeding NAF 4,000 (including linked transactions)
- Real-time risk alerts and investigation of flagged activities

Suspicious transactions are escalated and, where necessary, reported to the FIU. By combining automated detection with expert review, Company maintains a secure and compliant platform.

Simplified and Enhanced Due Diligence

Simplified Due Diligence (SDD)

SDD may be applied where the risk of ML/TF is minimal. Measures include:

- Collecting only basic personal details
- Delayed verification after account setup (where legally permissible)
- Reduced frequency of updates and lower-intensity transaction monitoring

SDD cannot be used if:

- Suspicious activity is detected
- The customer is high-risk

Enhanced Due Diligence (EDD)

EDD applies to customers presenting higher financial crime risks. Triggers include:

- Residence in high-risk jurisdictions
- PEP status
- Use of anonymous financial instruments (e.g., crypto, prepaid cards)
- Involvement in emerging financial technologies

EDD measures include:

- Collection of additional personal and financial data
- Detailed source of funds verification
- Transaction monitoring with automated alerts
- Senior management approval for high-risk relationships
- Verification of the first deposit from a regulated source

Timing of Due Diligence Procedures

Company applies CDD promptly, in accordance with regulatory thresholds.

Threshold-Based Verification

Customer identity is verified when:

- A single or cumulative transaction equals or exceeds NAF 4,000
- The customer reaches the threshold via deposit, withdrawal, or peer-to-peer activity

Before reaching this threshold, Company proactively verifies customer identities during registration to prevent misuse.

Restrictions While CDD is Pending

If the NAF 4,000 threshold is met and verification is incomplete:

- Further deposits/withdrawals are restricted
- Accounts may be frozen pending verification

If documents are not provided within 30 days:

- The business relationship is terminated
- Funds are returned to the original payment method (unless ML/TF is suspected, in which case they may be blocked)
- FIU is notified if suspicion of financial crime exists

Avoiding Tipping Off

Each case is handled carefully to avoid alerting customers to ongoing investigations, while ensuring compliance with AML/CTF laws.

Due Diligence for Existing Clients

CDD is not limited to new customers. Company monitors and reassesses existing clients on an ongoing basis to maintain compliance.

When re-verification is required:

- If a customer's risk profile changes (e.g., new jurisdiction, PEP designation)
- Following regulatory changes or legal triggers
- Upon reaching the NAF 4,000 transaction threshold

If past CDD was incomplete, Company prioritizes retrospective verification for high-risk clients, ensuring consistent compliance across all customer relationships.

Termination of Customer Relationships

Company terminates business relationships when:

- A player fails to comply with CDD requirements
- Suspicious financial activity is identified
- The customer is assessed as high-risk for ML/TF

Termination involves:

- Review and approval by senior management
- Final assessment of account history
- Reporting any red flags to the FIU
- Retention of records for a minimum of five years

This strict enforcement policy upholds the platform's security and compliance integrity.

Third-Party Reliance in CDD Processes

Company may utilize third-party services to carry out specific elements of the CDD process; however, it retains full responsibility for compliance.

Safeguards include:

- Immediate access to all customer identification data
- Written agreements outlining the third party's obligations
- Engagement only with regulated entities subject to AML/CFT supervision
- Independent risk assessments of the third party's jurisdiction

Third-party reliance differs from outsourcing:

- **Reliance** involves using independently gathered CDD data, with Company accountable for compliance.
- **Outsourcing** means the third party applies Company's internal CDD procedures under direct oversight.

All arrangements are subject to periodic review and audit to ensure regulatory standards are upheld.

23. Suspicious Activity Reporting

Company (Reg. Number: 141651) is fully committed to the timely identification and reporting of any activities that may be associated with money laundering (ML) or terrorist financing (TF). Indicators of such risks may include unusual client behavior, large or unexplained financial movements, or transactions involving high-risk jurisdictions. All employees are required to remain vigilant and report any concerns immediately to the appointed Compliance Officer.

Upon receiving a report, the Compliance Officer will conduct a detailed review to determine whether internal controls should be activated and whether the activity warrants formal reporting to relevant authorities, including the Financial Intelligence Unit (FIU).

Identifying Unusual Transactions

Transactions that deviate significantly from a customer's normal behavior or financial activity are classified as unusual. These may include:

- Large, uncharacteristic transfers of funds
- Dealings with unverified or unfamiliar third parties
- Transactions lacking a clear legal, economic, or legitimate purpose

Staff rely on automated monitoring tools and their training to flag such transactions, which are then forwarded to the Compliance Officer for further evaluation.

Transaction Types Subject to Reporting

In accordance with applicable regulations, **Company** considers the following types of transactions to be potentially suspicious and subject to further scrutiny:

1. Transactions Previously Flagged for ML/TF

Any transaction that has already been reported to law enforcement, the judiciary, or other authorities as potentially linked to ML or TF must automatically be treated as unusual.

2. Dealings Involving Sanctioned Individuals or Entities

Transactions involving persons or organizations listed under the **Sanctions National Ordinance (N.G. 2014 no. 55)**, or other applicable sanctions frameworks, are treated as suspicious and reviewed accordingly.

3. Transactions Equal to or Above NAF 5,000

Any financial activity—regardless of payment method—that meets or exceeds the NAF 5,000 threshold must be flagged. This includes:

- **Cash transactions:** Deposits or withdrawals at or above the threshold
- **Gaming-related purchases:** Acquisition of chips, tokens, or digital credits totaling NAF 5,000 or more
- **Payouts:** Redemption of winnings or other cash disbursements reaching or exceeding the same amount

This rule applies to both individual transactions and cumulative daily activity. Multiple transactions that collectively surpass NAF 5,000 within a single day must be assessed in totality.

If there is any reasonable suspicion—based on transaction behavior, customer profile, or contextual red flags—that the activity may relate to ML or TF, it must be treated as a **presumptively suspicious transaction** and escalated without delay.

Confidentiality in Reporting

To preserve the integrity of the suspicious activity reporting process and comply with legal obligations, **strict confidentiality** is maintained regarding all Suspicious Activity Reports (SARs). Employees must not inform the customer or any unauthorized third party about the filing of a SAR. This prohibition is essential to avoid **tipping off**, interfering with investigations, or compromising enforcement efforts.

Only authorized personnel—such as the Compliance Officer and designated members of the compliance team—are permitted access to SAR-related information. Staff are trained on the importance of discretion and the legal implications of confidentiality breaches.

Any violation of the confidentiality policy is treated as a serious compliance infraction and may result in disciplinary action, including termination. These measures ensure that Company's AML/CTF/CPF framework remains effective, secure, and fully aligned with legal and regulatory expectations.

By fostering a culture of awareness, accountability, and discretion, **Company** reinforces its dedication to regulatory compliance and strengthens its capacity to detect and report suspicious activities. This commitment supports broader efforts to combat financial crime and uphold the integrity of the iGaming sector.

24. Designated Compliance Officer

The **Compliance Officer** plays a vital role in safeguarding **Company** (Reg. Number: 141651) against risks related to money laundering (ML), terrorism financing (TF), and proliferation financing (PF). As the central authority within the company's AML/CTF compliance structure, the Compliance Officer is responsible for the design, implementation, and oversight of all anti-financial crime measures in accordance with Curaçao's legal framework and international regulatory standards.

A primary responsibility of the Compliance Officer is the development and continuous enhancement of the AML/CTF/CPF compliance program. This includes:

- Drafting and updating internal policies
- Ensuring alignment with national and international regulations

- Conducting regular evaluations to measure the effectiveness of compliance controls
- Advising senior leadership on regulatory developments and risk mitigation strategies

To foster a culture of compliance, the Compliance Officer organizes ongoing training programs for all employees. These sessions focus on emerging financial crime threats, regulatory updates, and practical guidance for recognizing and reporting suspicious activity.

In addition to policy management and training, the Compliance Officer oversees transaction monitoring and internal investigations. They are responsible for:

- Reviewing unusual financial activities
- Assessing transactions under the Ministerial Decree on Unusual Transactions
- Filing Suspicious Activity Reports (SARs) with the Financial Intelligence Unit (FIU)
- Deciding when account freezing or blocking is required to comply with anti-tipping-off laws

The Compliance Officer remains proactive in identifying regulatory risks and strengthening the AML/CTF/CPF framework. This includes:

- Monitoring global developments in financial crime prevention
- Recommending process improvements
- Providing management with periodic compliance reports summarizing risk findings, audit outcomes, and implementation progress

Through diligent oversight, training, and continuous refinement of compliance measures, the Compliance Officer ensures **Company** upholds a high standard of legal and regulatory integrity within the iGaming industry.

25. Independent Audit

To ensure full compliance with Curaçao's updated iGaming regulations, **Company** (Reg. Number: 141651) undergoes periodic **independent audits** of its Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) programs. These audits assess the effectiveness of the company's financial crime controls, identify areas for improvement, and verify alignment with both domestic and international regulatory expectations. The audit process is overseen by the **Curaçao Authority (CGA) Objective and Scope**

The main objective of the AML/CTF/CPF audit is to evaluate the robustness of Company's compliance framework. Regular audits enable the company to:

- Proactively identify weaknesses or gaps
- Strengthen internal risk controls
- Benchmark its program against industry best practices
- Demonstrate continued regulatory compliance

Audit reviews cover a broad range of compliance areas, including:

- Risk assessments
- Transaction monitoring systems
- Employee training programs
- Customer due diligence procedures

- Reporting and escalation protocols

Engagement of an Independent Auditor

To maintain impartiality, **Company** engages an external independent auditor—or in certain cases, a specialized internal team separate from the compliance function. The auditor’s qualifications, expertise in AML/CTF/CPF regulations, and independence are evaluated and approved by the **Curaçao Gaming Authority** prior to engagement.

Audit Components

Audits follow international compliance standards and GCB-issued guidelines, and include:

- **Policy & Procedure Review** – Evaluates whether AML/CTF/CPF policies are current, effective, and properly implemented
- **Risk Management Review** – Assesses the methodology for identifying and managing high-risk transactions, clients, and jurisdictions
- **Monitoring & Reporting** – Verifies that systems detect and report suspicious transactions accurately and in compliance with SAR obligations
- **Employee Training Review** – Assesses whether staff receive appropriate training on risk indicators, escalation procedures, and legal responsibilities
- **Customer Due Diligence Review** – Audits customer records for adherence to KYC, KYB, and CDD requirements
- **Reporting Mechanism Audit** – Reviews SAR filing procedures to ensure legal and procedural accuracy

Audit Findings and Follow-Up

Following the audit, the auditor prepares a comprehensive report summarizing findings, recommendations, and any identified deficiencies. This report is submitted to Company’s senior management and the **Curaçao Gaming Authority**.

In response, **Company**:

- Implements corrective actions within defined timelines
- Updates internal processes to close compliance gaps
- May be subject to follow-up audits to validate improvements

Regulatory Oversight by the Gaming Authority (CGA)

The GCB actively monitors licensed operators for compliance and may:

- Review submitted audit reports
- Request additional documentation
- Conduct site visits or interviews with senior management and the Compliance Officer
- Evaluate the implementation of audit recommendations

Consequences of Non-Compliance

Failure to meet AML/CTF/CPF obligations may result in:

- Monetary fines

- Temporary operational restrictions
- Suspension or revocation of the gaming license in cases of serious or repeated breaches

To mitigate these risks, **Company** maintains continuous communication with the GCB and takes a proactive approach to meeting all regulatory expectations.

Commitment to Compliance

By conducting regular, independent AML/CTF/CPF audits and ensuring full regulatory cooperation, **Company** demonstrates its ongoing commitment to financial crime prevention, operational transparency, and regulatory excellence. These audits form a critical part of the company's compliance strategy, helping maintain integrity and trust in its operations within the global iGaming ecosystem.

26. Management Responsibilities

At **Company**, strong governance begins at the top. The company's senior management and Board of Directors play a vital role in safeguarding the business from financial crime risks by actively overseeing all Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) efforts.

Management oversight is more than a regulatory obligation—it's a core part of Company's culture. The appointed AML/CTF/CPF Compliance Officer provides the Board with regular reports detailing changes in risk exposure, evolving regulatory requirements, and updates to the compliance framework. An annual effectiveness assessment ensures these safeguards remain robust, responsive, and aligned with global best practices.

To ensure policies stay current and effective, management conducts an annual policy review informed by monthly risk assessments. If vulnerabilities are identified, the Compliance Officer presents actionable recommendations to the Board for swift implementation. This ongoing review process reinforces Company's commitment to continuous improvement and regulatory excellence.

Training is another cornerstone of management responsibility. Company ensures all staff—especially those in sensitive or high-risk roles—receive relevant, ongoing compliance training. These programs empower employees to recognize red flags and respond to suspicious activity, fostering a company-wide culture of awareness and accountability.

Senior management also ensures strong internal controls through proper role segregation, clearly defined authorization protocols, and constant oversight. Documentation is meticulously maintained, ensuring transparency across all financial operations. In addition, independent audits are conducted regularly to evaluate and strengthen Company's AML/CTF/CPF framework—providing objective insights and helping the company stay ahead of compliance expectations.

27. Training & Record Keeping

Employee Training

At **Company**, knowledge is the first line of defense against financial crime. That's why the company has built a comprehensive AML/CTF/CPF training program to ensure every employee is equipped to detect and prevent suspicious activities.

Training is tailored to each role, with mandatory participation for all team members—from frontline support staff to senior executives. Whether monitoring transactions, verifying customer identities, or managing compliance reports, employees receive specialized instruction aligned with their responsibilities.

New hires undergo a full onboarding program that introduces them to Company's compliance obligations, internal procedures, and reporting expectations. All employees participate in mandatory refresher courses at least once per year, while those in high-risk roles—such as compliance officers and customer verification teams—receive additional, frequent training to stay ahead of emerging threats.

The curriculum covers a wide range of topics, including:

- Curaçao AML/CTF/CPF legislation
- Internal policies and compliance procedures
- Know Your Customer (KYC) and Customer Due Diligence (CDD) protocols
- Identification of suspicious transactions and red flag behaviors
- Record-keeping and reporting obligations
- Sanctions awareness and high-risk jurisdiction screening

Training sessions are delivered through engaging formats like workshops, webinars, e-learning modules, simulations, and real-life case studies. This hands-on approach ensures not just knowledge—but practical application.

Led by qualified internal experts and external consultants, the training content is continuously updated to reflect regulatory changes and global compliance trends. By investing in its people, **Company** builds a resilient, compliance-aware workforce that upholds the highest standards of integrity.

Record Keeping

Effective compliance depends on more than just knowing the rules—it requires impeccable documentation. At **Company**, record keeping is a top priority, forming the backbone of the company's AML/CTF/CPF compliance strategy.

The company maintains detailed records of:

- Customer identification and verification
- Transaction histories
- Suspicious Activity Reports (SARs)
- Training completion logs
- Internal audits and compliance assessments

In accordance with Curaçao's regulatory requirements, these records are retained for a minimum of **five years** and are readily accessible during audits or investigations.

Security is at the core of Company's record-keeping system. All data is encrypted and protected with strict access controls. Only authorized personnel have access, and every interaction is logged to ensure full accountability. Regular internal and external audits are conducted to verify data integrity and detect any vulnerabilities.

Company also uses a structured classification and retrieval system to ensure fast and accurate access to documentation when required. This efficiency supports both day-to-day operations and regulatory inquiries, reinforcing the company's reputation for transparency and compliance readiness.

By maintaining well-organized, secure, and auditable records, **Company** ensures full compliance with AML/CTF/CPF obligations while demonstrating its commitment to ethical, accountable business practices.

Appendixes

Appendix I

Player Risk Scoring Assessment

Risk Category	Question	Risk score	Risk level	Additional comments
Client	Customer's Age			
Geography	Customer's Citizenship			
Geography	Customer's Second Citizenship			
Geography	Customer's Country of Birth			
Geography	Customer's Country of Residence			
Client	Does Customer have the status of PEP/RCA (Politically Exposed Person/Relative and Close Associate)?			

HOW TO USE THIS?	
1. Only yellow and blue fields have to be filled.	
2. Comment section is available, however, it is not necessary for calculation of risk level.	
3. Majority of questions has dropdown list or checkbox. Correct answer(-s) should be selected	

NEW total score:	0.00
NEW risk level:	Low
Onboarding specialist:	
Last update date:	

Category	Score
low	0-1.5
medium	1.5-3.5
high	3.5 or more
unacceptable	

Risk Category:	To be:	Sum:	Weight:
Client	20%	0	
Geography	20%	0	
Products and Services	20%	0	
Transactions	20%	0	
Channels	15%	0	
Other	5%	0	
		0	

ACCOUNT PROFILE			
Client	Purpose of account registration?		
Client			
Client			
FUND SOURCE AND INCOME STATUS			
Client	Source of funds		average
Client			
Client			
Client			
Client			
Client	Source of wealth		average
Client			
Client			
Client			
Client			
INTENDED ACCOUNT ACTIVITY (DEPOSITS)			
Transactions	Average frequency of transactions		
Transactions			
Transactions	Expected total value of transactions per period (MAF)		
Transactions			
Transactions	Types of incoming payments		average
Transactions			
Transactions			
Transactions			
Transactions			
Transactions			
INTENDED ACCOUNT ACTIVITY (OUTGOING PAYMENTS)			
Transactions	Average frequency of transactions		
Transactions			
Transactions	Expected total value of transactions per period (MAF)		
Transactions			
Transactions	Types of outgoing payments		average
Transactions			
Transactions			
Transactions			
Transactions			
Transactions			
Transactions	Reasons for outgoing payments		average
Transactions			
Transactions			
Transactions			
GAMING BEHAVIOUR			
Please indicate services of interest			average
Products and Services			
Products and Services			
Products and Services			
Products and Services			
Products and Services			
Products and Services			
CONFIRMATIONS			
Payment Channels	Channels		average
Third-party Involvement			
Access			
Onboarding			
Client	Adverse media level		
Other	Manual risk level adjustment based on the expert judgement (±0.5):		
			Comment regarding manual risk adjustment: Summary of the applicant:

Appendix II

Employee Screening Program

This Employee Screening Program (“Program”) establishes the mandatory standards and procedures governing the vetting, assessment, and ongoing monitoring of all personnel employed or engaged by Pelican Entertainment B.V.

This Policy is adopted to ensure full compliance with CGA AML Regulation V.4, which requires firms to implement adequate screening procedures for employees both prior to employment and on an ongoing basis.

The Company further adopts an Employee Screening Checklist, which forms an integral part of this Policy and must be completed in all cases as evidence of adherence to the screening requirements set out herein.

This Policy applies to:

- All full-time, part-time, temporary, and contract employees.
- Senior Management, the Compliance Officer and all staff involved in AML/CTF obligations.
- Individuals engaged through third-party or outsourced arrangements performing regulated or sensitive functions.

No individual may commence employment or assume duties in a sensitive role until all screening measures required under this Policy have been satisfactorily completed.

Requirements

Pelican Entertainment B.V. shall ensure that all individuals are fit, proper, and suitable to perform their assigned duties. Screening procedures must be risk-based, proportionate to the sensitivity of the role, and documented.

The screening process consists of:

- (a) Pre-Employment Screening,
- (b) Fit-and-Proper Assessment (for designated roles),
- (c) Ongoing Screening, and
- (d) Completion of the Employee Screening Checklist.

Pre-Employment Screening

Human Resources (“HR”), in coordination with the Compliance Department, shall conduct the following mandatory pre-employment checks:

- Criminal Background Checks

A criminal record check shall be obtained to determine whether the applicant has been convicted of offenses relating to dishonesty, fraud, financial crime, money laundering, terrorist financing, or other conduct incompatible with the integrity expected of Company personnel.

- Verification of Identity

Applicants must present valid government-issued identification. HR shall verify identity authenticity and consistency.

- Verification of Academic and Professional Qualifications

All educational degrees, professional certifications, licenses, and other credentials relevant to the position must be independently verified.

- Employment History Verification

The Company shall confirm prior employment, roles, responsibilities, performance, and conduct, subject to applicable legal limitations.

- Reference Checks

At least two professional references must be obtained and documented. Adverse information must be escalated to Compliance for assessment.

Completion of the Employee Screening Checklist is mandatory before any offer of employment may be finalized.

Fit-and-Proper Assessment

A formal Fit-and-Proper Assessment shall be conducted to determine the individual's suitability for the role, evaluating the following:

- Integrity and Reputation

Absence of adverse regulatory findings, criminal convictions, ethical misconduct, or behaviour inconsistent with professional honesty.

- Competence and Professional Capability

Assessment of qualifications, technical skills, AML/CTF experience, and the capacity to discharge regulatory obligations.

- Financial Soundness

Where permitted by applicable law, consideration of financial history including bankruptcy, insolvency, or financial misconduct.

- Independence and Conflict of Interest

Assessment of the ability to act independently and without real or perceived conflicts of interest.

A Fit-and-Proper Assessment Form shall be completed, reviewed by the Compliance Department, and retained with the Employee Screening Checklist.

Ongoing Screening and Monitoring

Periodic Screening

Employees in sensitive, compliance-related, or high-risk roles shall undergo screening at least annually, including but not limited to:

- Updated criminal record checks (where legally permissible),
- Role suitability evaluations,
- Conduct and performance reviews,
- Confirmation of continued independence and absence of conflicts.

Trigger-Based Rescreening

Additional screening is required when:

- An employee is promoted or transferred to a sensitive role,
- Allegations or indicators of misconduct are identified,
- Regulatory or business changes increase the risk profile of the role,
- External information gives rise to concerns regarding fitness or propriety.

Continuous Conduct Monitoring

Supervisors and the Compliance Department must report any concerns regarding employee behavior or integrity for immediate assessment.

Mandatory Checklist Completion

For each periodic or trigger-based rescreening, the Employee Screening Checklist must be updated and retained.

Documentation and Record-Keeping

The Company shall maintain complete and accurate records of all screening activities, including:

- Background check reports,
- Verification evidence,
- Fit-and-Proper Assessments,
- Completed Employee Screening Checklists,
- Internal approvals and escalation notes,
- Any adverse findings and remedial actions taken.

Records shall be retained for not less than five (5) years, or longer where required by law or regulation, and shall be made available to competent authorities upon request.

Responsibilities

Human Resources

- Administers pre-employment screening and maintains screening files.
- Ensures completion of the Employee Screening Checklist.
- Escalates concerns to Compliance.

Compliance Officer

- Oversees screening for AML/CTF-related roles.
- Conducts Fit-and-Proper Assessments.
- Approves employment in sensitive roles.
- Ensures compliance with CGA Regulation V.4.

Senior Management

- Ensures adequate resources and oversight.
- Approves any exceptions or escalated cases.
- Reviews periodic compliance reports.

Compliance and Enforcement

Failure to comply with this Policy, including failure to complete the Employee Screening Checklist or Fit-and-Proper Assessment, may result in disciplinary action up to and including termination of employment.

The Company affirms that this Policy satisfies the requirements of CGA AML Regulation V.4 and shall review the Policy annually to ensure continued regulatory compliance.

Appendix III

Sanctions policy

Background

Pelican Entertainment B.V. is obliged to comply with laws imposing financial and other restrictions on dealings with certain entities, individuals and countries. This Sanctions Policy (hereinafter the “Policy”) sets out requirements and procedures designed to promote compliance with such laws (sanctions). Sanctions are a policy tool that national governments and multinational organisations use to constrain and deter perceived threats to their security, or to conform international conduct to recognised international standards. Sanctions arise in response to the conduct of countries, geopolitical rivals or transnational actors or trends. While national-level and multilateral sanctions regimes vary in content, rules, and restrictions, and the substance and frequency of enforcement action, they tend to fall into one of the below categories:

Conduct-based sanctions. These list-based sanctions, as described in an additional resource, are directed not at particular countries or governments but rather at anyone involved in defined types of malicious activity. Persons and entities can be designated for involvement in terrorism, proliferation of weapons of mass destruction, bribery/corruption, human rights violations, drug trafficking, organized crime, election interference, and cyber-enabled malicious activity. Conduct-based sanctions are meant to identify, disrupt, and deter sanctioned activities.

Special debt and/or equity sanctions. These relatively complex prohibitions allow for the continuation of day-to-day business with targeted entities while restricting the ability of targets to deal in new debt or new equity (valuable for, e.g., raising capital for long-term projects). These sanctions have generally been applied to entities within specific economic sectors (e.g., energy) but have also been applied to entities owned or controlled by a target government.

Sectoral sanctions. These sanctions target entities in a key sector or sectors of a country’s economy. Importantly, they may still allow for many ordinary business transactions with the country at issue, even with respect to the listed entities. The listed entities may not be themselves involved in targeted activity, but they may be identified due to their relationship to government decision-makers (to exert pressure on those decision-makers) or because of their importance to a country’s economy or future growth prospects.

Regime-based sanctions. These sanctions target current (or former) governments or regimes. They are not comprehensive: although they are associated with particular countries, they are primarily list-based, focused on officials involved in activity deemed to be a threat to national security,

economy, or foreign policy and on their associates. These sanctions tend to be paired with limited export controls or embargoes and related financing prohibitions. Most regime-based sanctions aim to protect human rights, combat state-sponsored or grand-scale corruption, and support democratic processes, institutions, and the rule of law.

Comprehensive sanctions. These sanctions target entire countries or geographic regions (e.g., the Crimea Region of Ukraine) and prohibit most activity involving those countries or jurisdictions. Comprehensive sanctions aim to alter government behavior by imposing economy-wide costs, restricting access to arms and tools of internal repression, and restricting access to a wide range of goods and services.

The key types of sanctions listed above may vary on the above characteristics even within a single category. Nor are these key types of sanctions mutually exclusive (e.g., regime-based sanctions may overlap with special debt and/or equity sanctions).

Sanctions Regimes. Due to the nature of the business of the Company, different regulatory regimes may have jurisdiction over its transactions, Clients, products and services. This section outlines the major sanctions regimes and the basis of their jurisdiction directly impacting the Company's operations.

The United Nations (UN). Under Chapter VII of the UN Charter, The United Nations Security Council (UNSC) can take action to maintain or restore international peace and security. The UN sanctions are administered by sanctions committees associated with the Security Council and are complemented by Financial Action Task Force (FATF) Recommendations 6 and 7. UNSC resolutions are legally binding to the UN member states.

The Company complies with sanctions restrictions imposed by the UN across all its operations.

The European Union (EU). Sanctions are one of the EU's tools to promote the objectives of the Common Foreign and Security Policy (CFSP): peace, democracy and the respect for the rule of law, human rights and international law. The EU implements all sanctions imposed by the UN. In addition, the EU may reinforce UN sanctions by applying stricter and additional measures. Where the EU deems it necessary, it may decide to impose autonomous sanctions.

EU restrictive measures only apply within the jurisdiction of the EU, that is: a) within EU territory, including its airspace; b) to EU nationals, whether or not they are in the EU; c) to companies and organizations incorporated under the law of a member state, whether or not they are in the EU. This also includes branches of EU companies in third countries; d) to any business done in whole or in part within the European Union; e) on board of aircrafts or vessels under the jurisdiction of a member state.

The Company complies with sanctions restrictions imposed by the EU across all its operations.

The United Kingdom (UK). The UK financial sanctions apply, inter alia: a) within the territory and territorial waters of the UK and to all UK persons, wherever they are in the world, b) to all individuals and legal entities who are within or undertake activities within the UK's territory, c) to all UK nationals and UK legal entities established under UK law, including their non-UK branches; they must also comply with UK financial sanctions that are in force, irrespective of where their activities take place.

The Company complies with sanctions restrictions imposed by the United Kingdom to the extent that such sanctions do not contradict the laws of the European Union.

The United States (US). In terms of applicability, the US sanctions fall into two categories:

- **primary US sanctions**; applicable to US persons, including all US citizens and permanent resident aliens regardless of where they are located, all persons and entities within the US, all US- incorporated entities and their foreign branches. In the cases of certain programs, foreign subsidiaries owned or controlled by U.S. companies also must comply. Certain programs also require foreign persons in possession of U.S.-origin goods to comply.
- **secondary US sanctions**: when applied, potentially subject non-U.S. persons to sanctions even if they are conducting business entirely outside of the United States and there is no US nexus in a relationship or a transaction. A number of sanctions programmes administered by the Office of Foreign Assets Control (OFAC) of the Department of the Treasury include secondary sanctions, including but not limited to Russia, Iran, Hong Kong/China sanctions programmes.

To the extent that is permissible under the local laws and the EU laws and regulations, the Company complies with both primary and secondary sanctions restrictions imposed by the US. Where compliance with secondary US sanctions is not permissible, e.g., regulation (EC) No 2271/96 and Joint Action 96/668/CFSP of 22 November 1996 protecting against the effects of the extra-territorial application of legislation adopted by a third country, and actions based thereon or resulting therefrom (OJ L 309, 29.11.1996, pp. 1 and 7), the Compliance Officer must escalate the matter to the Director(s) and the Board of Directors as a whole.

Policy Statement

Under this Sanctions Policy, the Company must:

- Where required by law, block accounts and other assets of sanctioned entities and individuals.
- In all other instances, prohibit or reject unlicensed trade and financial transactions with sanctioned jurisdictions, entities, and individuals.
- Exit relationships with Clients confirmed to be subject to sanctions, regardless of whether this is required by local law in the jurisdiction where the account or relationship is based. In the event that an exit is not permissible under local law, this should be escalated to the Director(s) and the Board of Directors as a whole.
- The Company must not knowingly engage in any transactions and/or business relationships structured to or aimed at the circumvention of applicable sanctions restrictions.

Failure to comply with this Policy may expose the Company to regulatory action or fines, civil or criminal liability as well as possible reputational damage.

Staff responsible for breaches of sanctions related laws and regulations may also be exposed to criminal liability or fines. Staff who fail to comply with this Policy may be subject to disciplinary action, including dismissal.

Roles and Responsibilities

The Board of Directors

The responsibilities of the Board of Directors with regard to the Company's Sanctions Policy shall include:

- Reviewing and approving this Policy as required.
- Ensures effective communication of the importance of sanctions compliance throughout the organisation.
- Provides oversight to ensure the AML/CTF and sanctions compliance function receives adequate support and resources at every organisational level and has sufficient authority and independence to effectively exercise its responsibilities.
- The Board receives and considers regular compliance reports presented by the Compliance Officer, covering both AML/CTF and sanctions compliance.
- Appointing a qualified Compliance Officer with overall responsibility for the proper application the sanctions policy and provides this senior-level officer with sufficient authority that when issues are raised they get the appropriate attention from the Board and the business lines.

The Director(s)

The Director(s) shall receive and evaluate regular compliance reports provided by the Compliance Officer and, where required, authorize changes based on the Compliance Officer's recommendations.

The Director(s) will also receive reports on particularly significant changes that may present risk to the Company as well as conflict of law and make the final decision regarding other sanctions-related issues escalated by the Compliance Officer as required by this Policy.

The Compliance Officer

The responsibilities of the Compliance Officer with regard to the Company's Sanctions Policy shall include:

- undertaking sanctions risk analysis of alerted transactions and/or potential and existing Clients including assessment of documentary evidence provided by Clients;
- proposing any necessary amendments to this Sanctions Policy and submitting them to the Board for approval;
- ensuring that all relevant employees are periodically informed of any changes in sanctions legislation, policies and procedures, as well as current developments and changes in sanctions evasion activities particular to their jobs;
- reviewing Client identification information to ensure that all the necessary information has been obtained.

All Other Employees

All Company employees should maintain continual awareness of the risk that sanctioned parties/transactions pose to the Company and its Client base and must not allow the Company to be used as a conduit for sanctions evasion. To support this, all staff are required to:

- Comply with this Sanctions Policy, related procedures, and applicable sanctions laws and regulations.
- Remain alert and promptly report to the Compliance Officer possible sanctions violations, or Clients found to be engaging in sanctions evasion activities or violations of this Policy or related procedures.
- Refrain from providing advice or other assistance to individuals or entities who seek to violate or attempt to violate any sanctions law or regulation, this Policy, or related procedures.
- Complete all required sanctions compliance training in a timely manner.
- In discussion or correspondence with Clients, staff are strictly prohibited giving any form of advice which might be seen as helping Clients to structure transactions or accounts in a way which could constitute sanctions evasion.

Sanction Screening

The Company must ensure that sanctions screening is performed on existing and prospective Clients, connected parties, transactions and third parties against sanction lists.

The specialized third party risk management solution selected by the Company shall ensure ongoing sanction screening process after a business relationship is established. The potentially matching data from various sanctions and watchlists is compared against the applicant profile to establish an exact match, before a match status is assigned. The following types of status may be assigned:

True positive: Applicant data exactly matches one or several watchlist records.

Potential match: Name of the applicant matches one or several watchlist records, but the age/year of birth data is missing, or the applicant is suspected of committing a crime.

False Positive: Applicant data does not match any of the watchlist records.

- Applicant data matches the watchlist record exactly, but additional information clearly shows that the applicant and the person on the record are different people.
- Applicant data matches the watchlist record, but the record does not include criminal or suspicious information about a person. For example, if the applicant is a crime journalist, and their name features on the article as the author.

Unknown: Applicant name in the document contains only one word.

Applicants with “True Positive” and “Potential Match” statuses are delegated to the Compliance Officer for further processing. If applicants are declined based on a watchlist match, they are assigned a respective rejection tag:

- Sanctions
- PEP

- Criminal records
- Adverse Media

In case of positive matches against sanctions lists, the action performed by the Compliance Officer will be in line with the requirements of a specific sanctions program (e.g. asset freeze, rejection, or debt/equity restrictions etc.) as well in consideration with any potential conflict of law.

Sanctions Evasion

UN, U.S., and EU sanctions programs include prohibitions on evasion of their principal provisions, with authorities increasingly focusing on evasion as its own category of sanctioned activity.

Examples of attempts to evade sanctions may include:

- Client (natural or legal person) who is not on any applicable sanctions list purchases cryptocurrency on behalf of a business entity owned by a sanctioned party.
- Where a payment is rejected by the Company, and the Client re-issues the payment after changing or removing information, thereby making it difficult to identify and restrict payments to and from sanctioned parties or countries (activity known as “wire stripping”).
- Client physically located in the U.S. utilizes VPN to mask IP address, thereby making it possible to engage in a transaction that is permitted in the EU but prohibited for the US Persons; or
- Payments to a party who is located in a non-sanctioned jurisdiction and acting as a “front company” or acting as an intermediary for sanctioned parties or parties in sanctioned jurisdictions.

Potential sanctions evasion activities may be detected by the Company’s staff at various levels of seniority and across different functions, i.e. through engagement with the existing or prospective Clients, business partners, transaction monitoring, ongoing due diligence (ODD) and other. All suspected attempts to evade or circumvent sanctions must be immediately escalated to the Compliance Officer who, after assessing the scenario, may decide that the case should be escalated to the relevant authorities.

In addition to sanctions screening, the Company utilizes its AML/CTF transaction monitoring, Client due diligence (CDD) and other processes to identify potential sanctions evasion activities by its Clients, third parties, and staff.

When performing the review and approval of Clients identified as high-risk according to the Company’s ML/TF risk assessment methodology, the Compliance Officer also reviews the Client for potential sanctions evasion activities.

The results of the investigation shall be recorded in line with the Company’s AML Policy. Potential sanctions evasion activities, if detected, must be included in the AML/CTF and sanctions compliance reporting documents submitted by the Compliance Officer to the Executive Director(s) and the Board.

Asset Freezing

For the purpose of this Policy, freezing, also known as “blocking”, refers to a form of controlling assets in which a sanctioned party has an interest. While title to blocked property remains with the sanctioned party, the exercise of the powers and privileges normally associated with ownership is prohibited without authorisation from the sanctioning competent authority. Blocking immediately

imposes an across-the-board prohibition against transfers or transactions of any kind with regard to the property.

“Assets” refer to tangible or intangible resources with economic value that an individual, corporation or country owns or controls with the expectation that it will provide future benefit. In case of the Pelican Entertainment B.V., the assets include cryptocurrency and fiat currency.

Sanctions Compliance Training

Sanctions compliance training is one of the pillars of the Company’s sanctions compliance program. The Compliance Officer is responsible for reviewing and updating (where required) the sanctions compliance program.

The compliance training falls under two categories:

1. Annual General Audience (All Staff) training,
2. Risk-Based/Ad-Hoc training to Staff who perform functions considered to be higher risk from a sanctions perspective, such as roles that entail Client contact, processing Client transactions, or otherwise evaluating Client data, must receive additional targeted training to supplement the annual sanctions learning provided to all Staff.

All Staff must receive annual General Audience (All Staff) sanctions compliance training. All new hires must receive the training within 30 (thirty) days of on-boarding. The General Audience (All Staff) sanctions compliance training shall include, at a minimum:

- Major sanctions regimes (UN, EU, UK, US).
- Major sanctions programs and requirements.
- Sanctions evasion methods and techniques.
- Sanctions risk indicators (‘red flags’).
- Sanctions compliance roles and responsibilities of the Company’s staff.
- Consequences of non-compliance.

All training records, including the training content (e.g. presentation slides, post-course assessment) and attendance records must be kept in line with the record-keeping requirements.

Outsourcing

Where a sanctions compliance activity is outsourced to an entity outside the Company, the Company is ultimately accountable for ensuring that such activities are undertaken in compliance with the requirements of this Policy, and all applicable sanctions laws, rules and regulations.

Record-Keeping And Record Retention

The Company adopts one set of record-keeping and record retention rules and requirements to all sanctions-related items as set by the Company’s AML Policy.

Appendix IV

Client Acceptance Policy

Statement of the Policy

Pelican Entertainment B.V. has implemented this Customer Acceptance Policy (“CAP”) to establish clear standards and procedures for assessing and approving customers who wish to access its online gaming and betting services. The purpose of this policy is to protect the company from being exploited for unlawful activities such as money laundering, terrorist or proliferation financing, sanctions evasion, fraud, and other illicit behaviour, while ensuring full compliance with Curaçao’s legal and regulatory framework.

This policy is aligned with the guidance of the Curaçao Gaming Authority and forms part of Pelican Entertainment B.V.’s wider Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and Counter-Proliferation Financing (CPF) program. It also incorporates international best practices, including the Financial Action Task Force (FATF) Recommendations, the European Union Anti-Money Laundering Directives, and the Wolfsberg Principles.

To comply with Curaçao legislation, the policy integrates the requirements of the National Ordinance on Identification when Rendering Services (NOIS), the National Ordinance on the Reporting of Unusual Transactions (NORUT), the Sanctions National Ordinance (SNO), the Kingdom Sanction Act, and the National Ordinance on Games of Chance (LOK).

This policy applies to all directors, officers, employees, contractors, and any third parties involved in onboarding and verification activities. No customer is allowed to deposit, withdraw, or engage in gaming activities until they have met all acceptance criteria and successfully completed the required identification, verification, and screening procedures.

2. Scope of the Policy

This policy applies to every individual or entity that wishes to open an account with Pelican Entertainment B.V., regardless of the registration channel used. This includes account creation through the company’s official website, mobile applications, affiliate partnerships, or third-party platforms.

The provisions of this policy cover the entire customer relationship, starting from the initial registration and continuing through all stages of account activity until closure or termination. It applies to all products and services provided by Pelican Entertainment B.V. under its Curaçao gaming license OGL/2024/427/1022

3. Customer Acceptance Integration

Pelican Entertainment B.V. only accepts customers who meet all applicable legal, regulatory, and internal compliance requirements. Every applicant must be verified to confirm they have reached the legal age for gambling, which is at least eighteen (18) years or higher where required by the laws of their jurisdiction. Applicants are also required to provide accurate and verifiable personal details, including their full legal name, date and place of birth, nationality, and current residential address.

The company does not allow the registration of customers who are residents of, located in, or conducting transactions from jurisdictions restricted under Curaçao's regulatory framework, international sanctions regimes, or Pelican Entertainment B.V.'s internal prohibited jurisdictions list. As part of the onboarding process, every applicant is screened against international and local sanctions lists, including those maintained by the United Nations, the European Union, the U.S. Office of Foreign Assets Control (OFAC), the U.K. Office of Financial Sanctions Implementation (OFSI), the Sanctions National Ordinance, the Kingdom Sanction Act, and any lists issued by the Curaçao Gaming Authority.

All funds used for gaming and betting activities must come from legitimate, lawful sources. Where the company's risk assessment indicates the need for additional scrutiny, customers are required to provide supporting documentation to verify the origin of their funds and, if applicable, their source of wealth. Pelican Entertainment B.V. also reserves the right to deny service to any individual or entity with a history of fraudulent behaviour, chargebacks, bonus abuse, self-exclusion due to problem gambling, or any other violation of gambling regulations.

4. Risk-Based Approach

Pelican Entertainment B.V. applies a thorough Risk-Based Approach (RBA) during both the onboarding process and the ongoing assessment of its customers. This approach ensures that the level of due diligence applied is proportionate to the customer's individual risk profile. The evaluation takes into account a range of factors, including the customer's personal and financial background, the types of products and services they use, any geographic risks associated with their location or funding sources, and potential risks arising from the technologies or channels they use to access the platform.

Customer Risk Profile

Pelican Entertainment B.V. assesses every prospective customer to determine their level of exposure to risks such as money laundering, terrorist financing, or proliferation financing. This assessment ensures that due diligence measures are applied proportionately to each customer's profile.

Customers who present clear, transparent, and verifiable financial backgrounds, for example, those with stable employment in low-risk sectors and gambling activity that aligns with their declared income are typically classified as low risk.

Conversely, customers may be considered high risk if they exhibit certain characteristics, such as having multiple or opaque income sources, employment in industries with elevated AML risk like cryptocurrency or unregulated financial services, or transaction patterns that appear inconsistent with their stated financial profile. Politically Exposed Persons (PEPs), their family members, and close associates are automatically categorised as high risk and are subject to stricter controls.

High-risk cases are managed through Enhanced Due Diligence (EDD), which may include more detailed verification procedures, additional documentation requirements, and ongoing monitoring. Examples of high-risk scenarios include:

- Customers with multiple or irregular income sources, who must provide evidence such as payslips, tax returns, business records, or investment statements.

- PEPs or their close associates, whose accounts require senior management approval, detailed source-of-wealth and source-of-funds checks, and ongoing enhanced monitoring.
- High or disproportionate spenders, where gambling activity exceeds what would reasonably match a customer's financial profile, requiring additional documentation and scrutiny.
- Customers exhibiting sudden, unexplained changes in gambling patterns or those using third parties to transact on their behalf, triggering immediate review and investigation.
- Attempts to operate multiple accounts, which are identified through internal monitoring systems and consolidated for a full transactional review.
- Unknown customers attempting to redeem large volumes of chips, or customers linked to junket operators, both of which require strict verification and EDD measures.

Pelican Entertainment B.V. also conducts ongoing monitoring to ensure customer risk profiles remain accurate and up to date. Periodic reviews are scheduled, and additional checks are triggered whenever significant changes are detected, such as unusual transaction patterns, large unexplained deposits, or changes to a customer's personal or financial circumstances. Where risk levels increase, the company applies enhanced controls including EDD, closer transaction monitoring, or restrictions on account activity to ensure risks remain effectively mitigated and regulatory obligations are consistently met.

Geographic Risk Assessment

Pelican Entertainment B.V. uses a dynamic geographic risk framework to evaluate potential risks linked to a customer's location or the origin of their funds. This framework is regularly updated based on trusted and authoritative sources, including publications and lists from the Financial Action Task Force (FATF), the Caribbean Financial Action Task Force (CFATF), the European Commission's high-risk country listings, the U.S. Office of Foreign Assets Control (OFAC), the U.S. Department of State's International Narcotics Control Strategy Reports, and Transparency International's Corruption Perceptions Index.

Customers from jurisdictions subject to international sanctions are not accepted under any circumstances. Those from high-risk jurisdictions may be considered for onboarding only after Enhanced Due Diligence (EDD) is completed and senior compliance approval is granted.

Jurisdictions are considered high risk when they exhibit one or more of the following characteristics: inadequate anti-money laundering and counter-terrorist financing frameworks or poor enforcement of such measures, systemic corruption that increases the likelihood of illicit funds entering the platform, association with international sanctions related to terrorism or weapons proliferation, or active presence of terrorist organizations.

To maintain accurate classifications, Pelican Entertainment B.V. continuously monitors relevant global and regional sources. These include FATF high-risk and monitored jurisdictions lists, CFATF advisories, the European Commission's list of countries with strategic AML/CFT deficiencies, OFAC sanctions lists, U.S. State Department reports, and corruption indices or reports indicating potential links to terrorist financing.

When a customer's country of residence or source of funds appears on a high-risk or sanctioned list, the case is escalated to the Compliance Officer. In such instances, EDD measures are mandatory, including in-depth identity verification, a thorough review of the source of funds and source of wealth, and enhanced transaction monitoring for as long as the relationship continues.

Geographic Risk Assessment Process

1. Initial Screening – The customer's location and funding sources are checked against global lists and reports to determine their risk level.
2. Low-Risk Jurisdiction – The account may be approved under standard due diligence procedures with routine monitoring.
3. High-Risk Jurisdiction – The application is escalated to compliance for review. Onboarding is only approved if all EDD criteria are satisfied, and heightened monitoring is applied.
4. Sanctioned Jurisdiction – The application is rejected, and records are retained in compliance logs.
5. Ongoing Monitoring – Customer profiles are dynamically updated, and additional controls are applied if jurisdictional risk changes over time.

Product, Service, and Transaction Risks

The level of risk associated with a customer is also determined by the products, services, and transaction types they use. Certain activities naturally carry a higher degree of risk due to reduced transparency and traceability. Examples include peer-to-peer transfers, the purchase or exchange of gaming tokens, or the use of anonymous or semi-anonymous payment methods such as prepaid cards or specific cryptocurrencies.

Accounts that are used mainly for financial transactions rather than genuine gameplay – such as those making large deposits followed by minimal or no betting activity before withdrawals – are treated with caution and subject to closer review. Likewise, the use of payment instruments not registered in the account holder's name automatically triggers additional verification measures to confirm legitimacy.

To mitigate these risks, Pelican Entertainment B.V. actively monitors and manages several key risk areas. Funds deposited into gaming accounts must always originate from lawful and verifiable sources. If there are signs that funds may be linked to criminal activities such as fraud, theft, or trafficking, customers are required to provide evidence of the legitimate source of those funds, and any suspicious transaction is reported to the Financial Intelligence Unit (FIU) in line with legal requirements.

Anonymous or semi-anonymous payment channels, including prepaid cards and certain virtual assets, are treated as high risk and subject to enhanced verification procedures, with full documentation of the source of funds. Accounts must also be used solely for genuine gaming purposes. Any behaviour suggesting misuse, such as depositing and withdrawing without significant gameplay, triggers an immediate review and may lead to account suspension during investigation.

Transactions involving third-party payment methods are flagged and subject to full verification of both the customer and the third party, including establishing the relationship between them and confirming the legitimacy of the funds. Similarly, transfers between gaming accounts are generally prohibited unless a legitimate and documented reason exists, in which case approval from the Compliance Officer is required, and full records of the transaction are maintained.

Operating multiple accounts or wallets – including those on different platforms under the company's control – is considered a red flag. Internal monitoring systems are designed to detect

and link related accounts, ensuring consolidated oversight and the ability to conduct a thorough review of all connected activity. Customers who frequently change their payment methods or banking details may also be attempting to obscure the origin of funds; such patterns prompt a detailed profile review and, where appropriate, the application of Enhanced Due Diligence (EDD).

Pelican Entertainment B.V. applies robust identity verification and authenticity checks to prevent and detect identity fraud. Any suspected cases are escalated to the relevant authorities in line with regulatory obligations. Additional controls are applied to the use of electronic wallets, particularly where providers are licensed in jurisdictions with weak AML or CTF oversight or where their structures make it difficult to trace funds. Customers using e-wallets are required to verify the source of their funds, and the provider's licensing and compliance standards are checked before any transaction is approved.

Channel and Technology Risk

The level of risk associated with a customer also depends on the channels and technologies used to access Pelican Entertainment B.V.'s services. Remote onboarding, while convenient, carries a higher risk of identity fraud or impersonation. To address this, the company relies on advanced digital Know Your Customer (KYC) solutions that include biometric verification, document authenticity checks, geolocation validation, and multi-factor authentication.

Before introducing any new technologies, payment solutions, or platform features, Pelican Entertainment B.V. conducts a comprehensive risk assessment to ensure the innovation cannot be misused for money laundering, fraud, or other illicit purposes.

Several factors are monitored closely to manage channel and technology-related risks. Any method that allows customers to remain anonymous is considered high risk and triggers enhanced verification measures. These measures include identity document validation, biometric checks, and real-time screening against sanctions and Politically Exposed Person (PEP) lists.

Remote interactions, although common in the industry and not inherently high risk, still demand strong safeguards. Pelican Entertainment B.V. uses secure verification technologies such as biometric checks, liveness detection, and automated document validation to prevent impersonation and fraud during onboarding and transactions.

When third parties are involved in customer interactions, the risk profile increases, especially if the intermediary is not subject to AML/CFT obligations. In such cases, Pelican Entertainment B.V. performs due diligence not only on the customer but also on the third party. This process includes verifying the intermediary's regulatory status, assessing its compliance framework, and ensuring all provided information is accurate and verifiable.

Risk Indicators

Pelican Entertainment B.V. applies a structured set of risk indicators to assess the level of risk associated with every customer relationship. These indicators form part of the company's Risk-Based Approach (RBA) and ensure that the level of due diligence applied is always proportionate to the customer's overall risk profile.

The evaluation covers multiple categories:

- **Customer Risk Profile** – factors such as multiple or irregular income sources, Politically Exposed Persons (PEPs), high or disproportionate spending, sudden changes in spending behaviour, involvement of third parties, multiple accounts, unknown chip redemptions, or links to junket operations.
- **Product, Service, and Transaction Risk** – warning signs such as proceeds of crime, anonymous or unregulated payment methods, misuse of accounts, third-party funding, frequent changes in payment instruments, identity fraud, or the use of multiple e-wallets.
- **Geographic Risk** – customers connected to jurisdictions with weak AML/CFT frameworks, high levels of corruption, international sanctions, terrorism links, or countries listed by FATF, CFATF, OFAC, or Transparency International's CPI.
- **Channel and Technology Risk** – customers accessing services through anonymous or unverified channels, onboarding remotely without sufficient identity validation, or relying on unregulated third-party intermediaries.

To determine the customer's overall risk, the company uses an internal Risk Calculator that assigns a weighted score to each indicator. The total score determines the customer's classification:

Risk Level	Requirements
Low Risk	Standard Customer Due Diligence (CDD) applies, with documentation limited to what is legally required or triggered by a change in risk profile.
Medium Risk	Standard CDD plus additional verification steps and closer ongoing monitoring.
High Risk	Full Enhanced Due Diligence (EDD), senior management approval prior to onboarding, and enhanced ongoing monitoring.

This risk-scoring approach ensures a consistent and methodical assessment of customers, allowing the company to allocate its resources effectively and meet its regulatory obligations.

Risk Indicators Table

Factor	Low Risk	Medium Risk	High Risk
Purpose of Account	Recreational or casual gaming.	Professional-level gambling or	Bonus exploitation or behaviour aimed at

		consistent high-stakes play.	financial abuse of promotions.
Source of Funds	Regular salary, savings, pensions, or other low-risk income.	Business income, legitimate casino winnings, sale of personal assets, inheritance, or documented loans/gifts from family or friends.	Unverified cryptocurrency, offshore accounts, or other unverifiable sources.
Source of Wealth	Long-term employment income, ownership of established businesses, verified inheritance, or steady investment growth.	Sale of property or business, significant lottery or gambling winnings.	High-risk investments such as cryptocurrency or forex trading, offshore holdings, or unverifiable assets.
Transaction Frequency	Occasional, typically monthly.	Regular, often weekly.	Frequent, typically daily.
Transaction Value (NAF)	Up to 1,000.	Between 1,000 and 4,000.	Over 4,000.
Incoming Payments	Standard bank transfers or debit/credit card deposits.	E-wallet or prepaid card deposits.	Cryptocurrency, third-party funding, deposits from high-risk jurisdictions, unusually high deposits, or use of unregulated processors.

Outgoing Payments	Normal withdrawals of winnings or deposit refunds.	Bonus-related cash-outs, frequent withdrawals, or large single withdrawals above 4,000.	Cryptocurrency withdrawals, third-party payments, chargebacks, or suspicious withdrawal patterns linked to other accounts.
Gaming Behaviour	Casual, moderate, and consistent play patterns.	Frequent high-stakes betting, extended play sessions, or fluctuating wagering amounts.	Aggressive betting patterns, rapid stake increases, loss-chasing, multiple accounts, collusion, or other fraudulent indicators.
Payment Channels	Traditional bank transfers.	Verified e-wallets.	Cryptocurrency or other anonymous or unverified payment methods.
Adverse Media	No negative information identified.	Questionable or unverified reports of misconduct.	Confirmed involvement in criminal or illicit activities.

Guidance on Using Risk Indicators

These indicators are designed to help staff assign an accurate risk profile to each customer during onboarding and throughout the customer relationship. Each factor should be assessed individually, and the combined results should inform the overall risk classification.

- Customers with mostly low-risk indicators are assigned a low-risk profile and subject to standard Customer Due Diligence (CDD).
- Customers with a mix of low and medium-risk indicators are classified as medium risk and require additional verification and closer monitoring.
- Customers displaying one or more high-risk indicators must undergo Enhanced Due Diligence (EDD), senior management approval before onboarding, and ongoing heightened monitoring.

Risk profiles should be reviewed regularly and adjusted when customer behaviour, transaction patterns, or external risk factors change. This approach ensures that the company's risk management remains dynamic and aligned with regulatory expectations.

5. Onboarding Procedures

Pelican Entertainment B.V. follows a structured and well-documented onboarding process to ensure that only customers meeting the company's acceptance standards gain access to the platform. No account is activated until the customer has successfully completed all required identification, verification, and sanctions screening steps.

During registration, customers are required to provide their full legal name, date and place of birth, nationality, residential address, and an official identification number such as a passport or national ID.

Every applicant is screened against international sanctions and Politically Exposed Person (PEP) databases using automated tools to ensure comprehensive coverage. Any potential matches or alerts are reviewed manually by trained compliance officers to confirm accuracy and rule out false positives.

If a customer is identified as high risk during the initial assessment, additional verification is required. This includes providing documentation to confirm the legitimacy of their funds and, where relevant, the source of their wealth. Acceptable documents may include recent bank statements showing income deposits, business account records or financial statements, tax returns, contracts of property or asset sales, and investment account statements. These enhanced measures ensure that the company meets regulatory expectations and maintains a strong control framework to protect the platform from misuse.

Client Identification requirements and verification procedures

This section refers to individuals who directly or indirectly establish a business relationship with the Company (e.g. direct Clients, beneficial owners, authorized persons, etc.). The Company should be satisfied that it is dealing with a real person and obtain sufficient evidence of identity to establish that a prospective Client is who he/she claims to be.

Document verification is intended to prevent the following issues:

- Forgery
- Data tampering
- Photo replacement
- Fraud
- Using document printouts
- Other manipulation

The ID document must contain as minimum the following information:

- Owner full name
- Owner full date of birth
- Document number
- Validity data (issue date or validity period)
- Owner photo

Owner signature (if applicable)

The ID document should meet the following requirements:

- The document is valid for at least one month from the upload date.
- The document is not scratched, stained, or torn.
- The applicant full name, date of birth and other important information is present and can be read.

Uploading the photo of an ID document

The photo of the ID document uploaded to the system should meet the following requirements:

The uploaded file is an original photo (static image) or scan (not a screenshot or a photo uploaded from social networks) in JPG, JPEG, PNG, PDF.

If the document has data on the front and back, both sides should be uploaded.

The size of the uploaded file is no less than 100 KB or 300 DPI.

The photo is in color.

The information in the document is readable.

All corners of the document are visible and no foreign objects or graphic elements are present.

The uploaded photo has not been edited with any software or converted to PDF.

The document is not digital (in most cases).

Checking the image for authenticity

The image authenticity check is intended to ensure that the uploaded image has not been edited electronically. This process involves automated signature analysis.

A software signature includes file metadata, compression parameters, vendor or software-specific tags, sections, and so on. An extensive database of camera and software signatures are utilized to determine the source of an image, detect traces of modification software, and estimate the risk of intended image tampering (as opposed to cosmetic changes like cropping, resizing, or rotation).

Document data validation

At the final step, the data extracted from the document is checked against various sources, including sanctions and watchlist databases.

1. Proof of address verification

a. Face-to-face procedures

For the purpose of face-face Client identification, the Compliance Officer shall inspect the person's original Proof of Address (PoA) documentation and make a certified true copy to be maintained as evidence of verification.

b. Non-face to face procedures

The process of Proof of Address (PoA) document verification for non-face to face Clients consists of the following steps:

- Uploading a PoA photo.

By default, the system accepts PoA documents that have been issued within the last 3 months.

- Checking the image for authenticity.

The image authenticity check is intended to ensure that the uploaded image has not been edited electronically. This process involves automated signature analysis.

A software signature includes file metadata, compression parameters, vendor or software-specific tags, sections, and so on. An extensive database of camera and software signatures are utilized to determine the source of an image, detect traces of modification software, and estimate the risk of intended image tampering (as opposed to cosmetic changes like cropping, resizing, or rotation).

Each image receives a digital trust score:

- Low – red (high risk of editing).
- Acceptable – yellow (there might be something to take a closer look at).
- Normal – green (a trusted and authentic image).

- Checking the integrity of the image.

Integrity checks are designed to ensure the uploaded image represents an official document by comparing it with a template from a database of original documents. Integrity checks consist of:

- General conformity to the template.
- Font originality and compliance with the relevant standards (width, spaces between the letters, and so on).
- Required fields and inscriptions.
- Data extraction (full name, home address, issue date).
- Data validation (whether the address is complete, if it exists and if it is really a home address).

To ensure the completeness and consistency of the extracted address data, external map services, such as Google Maps, Open Street Map, and others, are utilized allowing the Compliance Officer to see the applicant's geolocation in the Dashboard.

Supported PoA Documents

Common proof of residency examples:

- Tax bill (not older than 3 months).
- Mortgage statement.
- Certificate of voter registration.
- Correspondence with a government authority regarding the receipt of benefits such as a pension, unemployment benefits, housing benefits, and so on.

- Cable internet/TV bill (but not from satellite TV companies or for other wireless telecommunication services).
- Landline telephone bill.
- Bank statement with the date of issue and the name of the person (the document must be not older than 3 months).
- Utility bill for gas, electricity, water, internet, etc. linked to the property (the document must not be older than 3 months).
- A lease agreement that is current and has the signatures of the landlord and the tenant.
- Rent bills issued by a real estate rental agency.
- Credit card statement issued by a bank.
- Letter from a recognized public authority or public servant (any government-issued correspondence not older than 3 months).
- Employer's certificate for PoA.
- House purchase deed.
- The document must contain the full name, home address, and the document issue date (in most cases). Both paper documents and electronic documents (in PDF) are accepted.

Alternative proof of residency examples

The following documents can also be accepted as valid PoA, but only if they contain an address:

- Passport
- Identity card
- Driving license
- Residence permit (EU samples containing address)

**** The same document cannot be used to confirm both an identity and a place of residence. So, if an applicant submits an ID document as PoA, they should use another document to confirm their identity.*

Documents which are not acceptable as Proof of Address, include:

- Old government-issued correspondence (older than 3 months)
- Old bank statements (older than 3 months)
- Old utility bills linked to the property (older than 3 months)
- Pension statements
- Bank references
- Insurance policies
- Mobile phone bills
- Medical bills
- Receipts for purchases
- Insurance statements
- Documents stating PO Box addresses
- Checks
- Envelopes and parcels showing your name and an address

- Prepaid card invoices
- Mobile sim cards+ bills issued to a business address
- Bills from debt collection agencies
- Bills from fintech companies
- Papers referring to discount cards which cannot be considered as bank cards
- Car rent bills

Source of Funds (SoF) and Source of Wealth (SoW)

SoF refers to origin of funds being deposited, received, or transferred with the Company. SoF tells us where the money is coming from, which can be proven through bank statements, tax returns or the Company financials, etc.

Typically, SoW is requested when establishing business relationships or performing EDD, SoF is requested when there is a need to understand what the origin of a transaction is.

6. Ongoing Monitoring

Pelican Entertainment B.V. recognises that customer acceptance is an ongoing process rather than a one-time activity. Continuous monitoring is essential to ensure that customer behaviour remains consistent with the profile established during onboarding and that any irregularities or deviations are promptly identified and addressed.

The company uses automated transaction monitoring systems to detect patterns of unusual or suspicious behaviour. Alerts are generated for activities such as deposits or withdrawals that do not match the customer's declared profile, rapid movement of funds without meaningful gameplay, the use of multiple or unusual payment methods, or patterns that may suggest collusion, chip-dumping, or other prohibited activities.

Each alert is reviewed by trained compliance officers, who assess the circumstances and determine whether further investigation or escalation is needed.

In addition to real-time monitoring, the company conducts periodic reviews of customer profiles on a risk-based schedule to ensure risk ratings remain accurate. If there are material changes in a customer's situation, such as relocation to a high-risk jurisdiction, significant increases in transaction values, or changes in funding methods, the customer's risk profile is immediately reassessed. Where necessary, enhanced monitoring and other controls are applied to maintain compliance and mitigate potential risks.

7.Prohibited clients and transactions

Certain types of Client/transactions are not accepted for establishing business relationships or conducting transactions in order to reduce the risk that the services and products of the Company may be used for money laundering or terrorist financing or other illicit purposes and at the same time for protect the Company from the financial, reputational and legal risks.

Consequently, it is strictly prohibited to:

- c. Establish a business relationship with Clients who fail or refuse to submit the requisite data and information for the verification of their identity and the creation of their economic profile, without adequate justification.
- d. Establish a business relationship and/or conduct transactions with natural or legal persons against which sanctions prohibiting such relationship/transactions are imposed in accordance to the Company's Sanctions Policy (Appendix II).
- e. Conclude or implement any business relationship with a credit institution or other financial institution or an institution that carries out activities equivalent to those carried out by credit institutions and financial institutions or legal person that is incorporated in a jurisdiction in which it has no physical presence, involving meaningful management and which is unaffiliated with a regulated financial group (i.e. shell company) or is known to permit accounts to be held by a shell bank.
- f. Establish a business relationship or conduct transactions that involve in any way, directly or indirectly, natural or legal persons whose activities are related to criminal activity including (but not exhaustive)
 - Terrorist offences, offences related to a terrorist group and offences related to terrorist activities as set out on Titles II and III of Directive (EU) 2017/541 (replacing Framework Decision 2002/475/JHA on combating terrorism)
 - Any of the offences referred in article 3(1)(a) of the 1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances;
 - The activities of criminal organizations as defined in Article 1(1) of Council Framework Decision 2008/841/JHA on the fight against organized crime;
 - Trafficking in human beings and migrant smuggling, including any offence set out in Directive 2011/36/EU;
 - Sexual exploitation, including any offence set out in Directive 2011/93/EU;
 - Fraud affecting the Union's financial interests, where it is at least serious, as defined in Article 1 (1) and Article 291) of the Convention on the protection of the European Community's financial interests;
 - Corruption, including any offence set out in the Convention on the fight against corruption involving officials of the EU Communities or officials of Member States of the EU;
 - Counterfeiting of currency, including any offence set out in Directive 2008/99/EC;
 - Cybercrime, including any offence set out in the Directive 2013/40/EU;
- g. Establish a business relationship or conduct transactions that involve in any way, directly or indirectly, natural or legal persons where:
 - Legal entities are owned through bearer instruments;
 - Legal entities are involved in the adult industry;
 - Legal entities are involved drugs industry;
 - Legal entities are involved in arms industry;
 - Specially Designated Nationals and Blocked Persons (SDNs);
 - Clients acting on behalf of Specially Designated Nationals and Blocked Persons (SDNs);
 - Clients whose source of funds (SoF) and source of Wealth (SoW) were generated from a sanctioned activity;

- Clients whose source of funds (SoF) and source of Wealth (SoW) cannot be verified when this is required;
- Purchase or sale of virtual assets ultimately owned or controlled, directly or indirectly, by sanctioned parties;
- Transactions with third parties ultimately owned or controlled, directly or indirectly, by sanctioned parties;

8. Enhanced Due Diligence (EDD)

Enhanced Due Diligence (EDD) procedures are applied to customers who present an elevated risk profile. This includes Politically Exposed Persons (PEPs), their family members, and close associates; customers based in or funding their accounts from high-risk jurisdictions; those conducting unusually large, complex, or unexplained transactions; and customers whose financial behaviour is inconsistent with their declared income or business activities.

EDD involves a more detailed and rigorous verification process than standard due diligence. This includes a full analysis of the customer's source of funds and source of wealth, supported by credible and independent documentation. Additional steps include corporate registry and public record searches to verify legal and beneficial ownership, confirmation of employment or business ownership, reviews of audited financial statements or other reliable financial documents, and thorough adverse media and reputational checks.

Senior management approval is required before onboarding any high-risk customer, and in complex or sensitive cases, formal approval from the Board of Directors may be necessary.

Once these customers are onboarded, they are subject to ongoing enhanced monitoring. This includes lower thresholds for triggering transaction reviews, closer scrutiny of their transaction patterns, and more frequent reassessments of their risk profiles. These measures ensure that higher-risk relationships are managed appropriately, in full alignment with both regulatory obligations and the company's internal risk appetite.

Prohibited Customer Categories

Pelican Entertainment B.V. will not onboard or will immediately terminate relationships with customers who meet any of the following criteria:

- Anonymous or unverifiable customers, including those who fail or refuse identity verification within 30 days.
- Shell companies, fictitious entities, or customers with unclear beneficial ownership.
- Sanctioned individuals or entities, including those appearing on UN, EU, OFAC, OFSI, SNO, or Kingdom Sanction Act lists.
- Residents of or transacting from prohibited or sanctioned jurisdictions, as defined in Section 4 (Geographic Risk).
- Customers below the legal age for gambling.
- Customers involved in fraud, bonus abuse, identity theft, or other illicit behaviour.
- Third-party transactors or users of anonymous payment channels without valid justification or verification.
- Customers whose source of funds or source of wealth cannot be verified or is linked to crime.

Acceptance and Rejection Triggers

Customer applications will be immediately rejected or suspended when any of the following triggers occur:

a. Documentation and Verification Failures

- Refusal to provide KYC, proof of address, or EDD documentation.
- Submission of false, altered, or misleading information.
- Failure to complete mandatory verification within 30 days.

b. AML/CTF/CPF Risk Triggers

- Positive sanctions match or verified PEP hit without manageable risk.
- Suspicion of money laundering, terrorist financing, proliferation financing, or other criminal activity.
- Inability to verify SOF/SOW after reasonable attempts.

c. Behavioural and Transactional Triggers

- Highly unusual deposit/withdrawal activity inconsistent with profile.
- Multiple accounts, third-party payments, or misuse of payment instruments.
- Attempts to circumvent controls or operate through intermediaries.
- Evidence of collusion, chip dumping, or non-genuine gameplay.

9. Termination

Pelican Entertainment B.V. reserves the right to suspend or terminate any customer relationship when required by regulations, internal policies, or risk considerations. This action may be taken if a customer fails to provide the requested identification or supporting documentation within 30 calendar days, if there is reasonable suspicion of money laundering, terrorist financing, or proliferation financing, or if the customer engages in activities that violate applicable laws, regulations, or the company's Responsible Gambling Policy.

When a relationship is terminated due to suspected criminal activity, the company promptly files a report with the Financial Intelligence Unit (FIU) in accordance with the National Ordinance on the Reporting of Unusual Transactions (NORUT). Any remaining funds in the account are returned to the original funding source unless there is a legal requirement to freeze or seize the funds pending investigation. Detailed records of all termination actions, including the rationale and supporting evidence, are maintained for at least five years.

Pelican Entertainment B.V. will refuse to onboard or will terminate an existing relationship in cases where:

- The customer is a resident of, located in, or conducting transactions from a prohibited or sanctioned jurisdiction.
- The customer fails to provide required information or documentation within the specified timeframe.
- False, misleading, or incomplete information is provided during registration or verification.
- The source of funds or source of wealth cannot be confirmed as legitimate.
- The customer is involved in, or suspected of, money laundering, terrorist financing, or other criminal activity.
- The customer is a Politically Exposed Person (PEP) whose risk profile cannot be mitigated to an acceptable level.

Fraudulent activities, bonus abuse, collusion, or prohibited gambling behaviour are detected.

- The customer attempts to use third parties to transact without proper disclosure and verification.
- The customer has self-excluded or been excluded for responsible gambling reasons.
- Large chip redemptions or withdrawals are requested without verifiable linked gambling activity.
- The customer is a minor or below the legal gambling age in their jurisdiction.

10. Curaçao's Legislative Framework

Pelican Entertainment B.V. acknowledges that its Customer Acceptance Policy is an integral part of its wider Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and Counter-Proliferation Financing (CPF) framework. The policy is designed to fully comply with Curaçao's legal and regulatory requirements, including the National Ordinance on Identification when Rendering Services (NOIS), the National Ordinance on the Reporting of Unusual Transactions (NORUT), the Sanctions National Ordinance (SNO), the Kingdom Sanction Act, and the National Ordinance on Games of Chance (LOK).

Compliance with these obligations is treated as a priority in daily operations. The customer acceptance procedures are embedded within the company's compliance processes to ensure due diligence is continuous and extends beyond onboarding. This approach ensures that any significant changes in a customer's risk profile, transactional behaviour, or jurisdiction are identified and addressed promptly.

All employees involved in onboarding and verification activities receive dedicated training to help them understand the legislative framework and the company's internal standards. The training focuses on effectively applying the Risk-Based Approach, identifying and escalating high-risk indicators, and following escalation protocols to the Compliance Officer or senior management.

Independent audits are conducted at least annually to evaluate how effectively the Risk-Based Approach and the Customer Acceptance Policy are being implemented. These audits review critical processes, such as identity verification, sanctions and PEP screening, Enhanced Due Diligence (EDD) procedures, and the ongoing monitoring of customer activities. The findings are reported to the Board of Directors, and any gaps or deficiencies are addressed promptly through corrective measures implemented within defined timeframes.

11. Responsible Gambling Integration

Pelican Entertainment B.V. ensures that its Customer Acceptance Policy is fully aligned with its Responsible Gambling Policy, recognising that protecting customers from gambling-related harm is a key part of its compliance and operational framework.

If a customer shows behaviour that indicates potential harm, such as frequent deposits that exceed their apparent financial capacity or excessively long gaming sessions, the company takes immediate action. Depending on the situation, this may include setting deposit or wagering limits, temporarily suspending the account, or, in severe cases, refusing further access to services to protect the customer.

Self-exclusion requests are handled promptly and applied to all accounts linked to the customer to ensure these measures cannot be bypassed. These restrictions remain active for the period specified by the customer or as required by regulatory standards.

Employees in customer-facing roles receive targeted training to help them identify early signs of problem gambling. This training is incorporated into both the onboarding process and ongoing monitoring activities, enabling timely intervention when risk indicators are observed.

12. Review and Governance of CAP

This Customer Acceptance Policy (CAP) is reviewed at least once every twelve months to ensure that it remains effective, compliant with legislative and regulatory requirements, and consistent with industry best practices. The review process also takes into account any changes to the company's risk profile, emerging patterns in customer behaviour, and technological advancements that could create new risks or vulnerabilities.

Proposed revisions or updates are prepared by the Compliance Officer and submitted to the Board of Directors for approval prior to implementation. All updates are thoroughly documented, and relevant staff are informed and trained to ensure that the revised policy is applied consistently and accurately throughout the company's operations.

13. Record Keeping

Pelican Entertainment B.V. keeps detailed records of all customer acceptance activities for at least five years after the end of the business relationship, in accordance with regulatory requirements. These records include identification and verification documents, proof of address, evidence of the source of funds and source of wealth, transaction monitoring alerts and investigation reports, Enhanced Due Diligence (EDD) files, internal compliance reviews, and documentation of any account suspensions or terminations.

All records are stored securely in encrypted formats with strict access controls to ensure confidentiality and data protection. Only authorised personnel have access to these records, and all access activity is logged and periodically reviewed to verify compliance with internal policies and applicable data protection regulations.

Appendix V: 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 buitengaats 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).