

Pelican Entertainment B.V.

registration number: 134359

license number: OGL/2024/561/0554

Dr. H. Fergusonweg 1, Curaçao

Customer Acceptance Policy

Date:	17.09.2025
Version:	1.0
Approved by the Board of Directors:	

Effective Date: 23 September 2025

Next Review Date: 22 September 2026

Document Outline

1. Policy Statement and Scope
2. Compliance with Curaçao's Regulatory Framework
3. Customer Acceptance Requirements
4. Risk-Based Compliance Framework
 - 4.1 Assessing the Customer Risk Profile
 - 4.2 Product, Service, and Transaction-Related Risks
 - 4.3 Geographic Risk Assessment
 - 4.4 Channel and Technology Risks
 - 4.5 Risk Indicators
5. Onboarding Process
6. Enhanced Due Diligence
7. Ongoing Monitoring
8. Relationships Termination
9. Responsible Gambling Integration
10. Record Keeping
11. Policy Review and Approval

1. Policy Statement and Scope

Pelican Entertainment B.V. has adopted this Customer Acceptance Policy to set the standards, procedures, and criteria for approving customers on its online gaming and betting platform. Its purpose is to prevent the company from being misused for money laundering, terrorist or proliferation financing, sanctions evasion, fraud, and other illicit activity, while ensuring full compliance with Curaçao's regulatory framework, including (without limitation) 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).

The policy aligns with guidance issued by the Curaçao Gaming Control Board and forms an integral part of Pelican Entertainment B.V.'s broader Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and Counter-Proliferation Financing (CPF) framework. It also reflects internationally recognised standards, including the Financial Action Task Force (FATF) Recommendations and the European Union Anti-Money Laundering Directives.

This policy applies to all directors, officers, employees, contractors, and third parties involved in customer onboarding and verification. Customers may not deposit, withdraw, or place bets until they meet the acceptance criteria and complete all required verification and screening procedures.

The policy covers every individual or entity seeking to register an account with Pelican Entertainment B.V., regardless of the channel used whether via the company's website, mobile applications, affiliate networks, or third-party platforms.

The policy governs every stage of the customer lifecycle, from initial application and onboarding, through ongoing relationship maintenance (periodic reviews and account monitoring), to account closure or termination. Its standards apply without exception to all products, services, and gaming activities offered by Pelican Entertainment B.V. under Curaçao licence OGL/2024/561/0554.

2. Compliance with Curaçao's Regulatory Framework

Pelican Entertainment B.V. recognises that its Customer Acceptance Policy (the "Policy") is a cornerstone of the company's enterprise-wide financial crime compliance framework, encompassing Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and Counter-Proliferation Financing (CPF). The Policy sets binding principles, controls, and procedural standards for customer identification and verification, risk assessment, customer due diligence (CDD) and enhanced due diligence (EDD), ongoing monitoring, sanctions and politically exposed person (PEP) screening, record-keeping, and escalation. It has been designed to ensure full consistency with Curaçao's legal and

regulatory requirements, including, without limitation: 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).

Meeting these obligations is fundamental to Pelican Entertainment B.V.'s day-to-day operations. Customer acceptance controls are integrated into the company compliance framework so that due diligence is continuous, beginning at onboarding and persisting throughout the customer lifecycle. It enables timely detection and mitigation of any significant shifts in a customer's risk profile, behaviour, or jurisdiction.

All employees involved in customer onboarding and verification must receive tailored training that addresses both regulatory obligations and Pelican Entertainment B.V.'s internal controls. The training emphasises implementing a Risk-Based Approach, spotting high-risk indicators, and adherence to established escalation procedures involving the Compliance Officer or senior management.

Pelican Entertainment B.V. engages independent auditors at least once a year to maintain strong governance and regulatory alignment. These reviews assess the effectiveness of the Risk-Based Approach and the consistent application of the Customer Acceptance Policy, with examinations covering identity verification, sanctions and PEP screening, EDD, and ongoing transaction monitoring. Findings are reported to the Board of Directors, and any weaknesses are promptly addressed through structured corrective action plans, ensuring continuous compliance and resilient operations.

3. Customer Acceptance Requirements

Only customers who fully comply with legal, regulatory, and internal standards are accepted by Pelican Entertainment B.V. Eligibility requires confirmation of legal gambling age, the applicant must be at least eighteen (18) years old, or older if required by local law. Applicants are required to submit complete, accurate, and verifiable personal data, including their full legal name, date and place of birth, nationality, and current residential address.

The company does not admit customers located in, attempting to access from, or transacting within jurisdictions subject to restrictions under Curaçao law, international sanctions, or Pelican Entertainment B.V.'s prohibited-country list. All applicants (and, where relevant, beneficial owners and authorised users) are screened against the United Nations, the European Union, the U.S. Office of Foreign Assets Control (OFAC), the U.K. Office of Financial Sanctions Implementation (OFSI), and lists issued pursuant to Curaçao's Sanctions National Ordinance and Kingdom Sanction Act, as well as any directives of the Curaçao Gaming Control Board.

Funds used for gaming and betting activities must be derived only from lawful, verifiable sources. When a customer's risk profile triggers enhanced due diligence, Pelican Entertainment B.V. may require further substantiation of source of funds and, where needed, source of wealth. Services may be declined or curtailed for applicants or customers associated with fraud, multiple chargebacks, bonus abuse, infringements of gambling laws, or earlier self-exclusion on problem-gambling grounds.

4. Risk-Based Compliance Framework

The company applies a structured Risk-Based Approach (RBA) across both the customer onboarding process and the ongoing monitoring of existing relationships. This approach calibrates the breadth and depth of due diligence to the individual risk profile. The assessment considers personal and financial background, the nature of the products and services being used, geographic exposure, and risks associated with the technologies or channels employed.

4.1 Assessing the Customer Risk Profile

The company assesses every prospective customer to determine their exposure to risks such as money laundering, terrorist financing, or proliferation financing. The outcome of this assessment sets the customer's risk rating and ensures that due-diligence measures (CDD/EDD) are proportionate to that rating.

- **Low risk customers**

Customers are classified as low risk when they have clear, verifiable income, maintain stable employment within sectors assessed as low risk, and their wagering/transaction activity is consistent with their stated financial profile.

- **Medium risk customers**

A Medium-risk classification applies when one or more factors are present: (i) legitimate but less easily verifiable income; (ii) employment in sectors with moderate exposure to financial-crime risk; or (iii) activity that intermittently conflicts with the declared financial profile. Such customers receive standard Customer Due Diligence (CDD) supplemented by additional verification measures and increased monitoring.

- **High risk customers**

Customers are rated high risk where one or more factors are present: (i) complex or non-transparent sources of income; (ii) employment in industries associated with higher money-laundering or terrorist-financing risk (such as crypto

businesses or unregulated financial services); or (iii) activity inconsistent with the declared financial profile. Politically Exposed Persons (PEPs) including their immediate family members and close associates fall into this category. Such relationships require Enhanced Due Diligence (EDD) more intensive checks, collection of supplementary evidence, and ongoing activity monitoring.

Key indicators requiring enhanced scrutiny

- **Politically Exposed Persons (PEPs):** PEPs and their close associates are automatically classified as high risk. They are subject to enhanced verification of source of wealth and source of funds, must obtain senior-management approval prior to account opening, and are monitored continuously.
- **Customers Linked to Junket Operators:** Customers connected to junket operators are deemed high risk. Enhanced Due Diligence (EDD) is required for the customer and the operator, with specific attention to financial relationships and the provenance of funds.
- **Complex or Unclear Earnings.:** Customers earning from multiple or opaque sources must provide supporting evidence for each, such as payslips, tax returns, business records, or investment documentation. Where earnings are volatile or inconsistent, the company will request additional documents to confirm legitimacy and will apply continued monitoring.
- **High-Value or Inconsistent Activity:** Spending that is out of proportion to the customer's declared income triggers additional verification and documentation. Unusually large or frequent betting requires documented proof of lawful source of funds (e.g., bank statements, payslips, tax returns, sale proceeds).
- **Sudden Behavioural Changes:** Unexplained changes in wagering behaviour, particularly by casual/tourist customers, will result in elevation to higher risk status and intensified oversight.
- **Third-Party Involvement:** Any attempt to deposit, withdraw, or place bets via a third party is flagged for immediate investigation, and all involved parties are subjected to verification.
- **Multiple or Linked Accounts:** Operating more than one account is considered suspicious. Any linked accounts will be consolidated and subjected to a full compliance review.
- **Fund Redemption without Activity:** Customers requesting significant redemptions without commensurate, verifiable wagering activity must first complete identity verification and source-of-funds checks before any payout is processed.

Ongoing monitoring

The company continuously monitors customer behaviour to ensure risk profiles remain current and accurate. Reviews are carried out on a risk-based schedule and may also be

triggered by material changes, such as unusual transaction patterns, large unexplained deposits, or updates to personal or financial information. If a customer's risk rating increases, the company applies additional safeguards such as Enhanced Due Diligence (EDD), heightened transaction monitoring, or limits on account activity. This adaptive framework ensures risks are managed effectively and remain aligned with regulatory requirements.

4.2 Risks Related to Products, Services, and Transactions

A customer's risk profile reflects not only their background but also the products, services, and transaction patterns they use. Activities with limited transparency, weaker audit trails, or higher misuse potential such as peer-to-peer transfers, purchasing or exchanging gaming tokens, and funding via anonymous or semi-anonymous instruments (e.g., prepaid cards or selected cryptocurrencies) are treated as higher risk.

Transaction patterns indicating that an account is used primarily to move funds rather than for genuine gaming, for example, substantial deposits followed by minimal betting and rapid withdrawals - are treated as red flags and trigger enhanced scrutiny. The use of payment methods not registered to the account holder is likewise considered suspicious and requires additional verification before processing.

The company applies ongoing monitoring to detect and mitigate the key risks within this area:

- **Identity Fraud:** The use of stolen or fabricated personal or financial information to open or fund gaming accounts poses a significant risk. The company applies strict verification and authenticity checks to detect and prevent such activity, with suspected incidents escalated and reported to relevant authorities.
- **Anonymous and High-Risk Payment Methods:** Deposits made through prepaid cards, cryptoassets, or similar low-traceability instruments are classified as high risk. Users of these methods are subject to enhanced verification and must evidence the legitimate origin of funds.
- **Electronic Wallets:** Certain e-wallet providers operate in jurisdictions with weak AML/CTF oversight or permit anonymous cash top-ups, increasing their vulnerability to misuse. Fund flows may remain opaque even with regulated providers if banking records only show transfers to the wallet. Accordingly, customers must evidence lawful funding, and the company will review the provider's licensing and regulatory framework before enabling this payment method.
- **Frequent Changes in Payment Methods:** Customers who repeatedly switch bank accounts or payment instruments may be attempting to obscure the origin of funds. Such activity triggers a detailed profile review and, the application of Enhanced Due Diligence (EDD) where necessary.

- **Transfers Between Accounts:** Transfers between gaming accounts are prohibited. Exceptions must be authorised by the Compliance Officer, complete documentation, and appropriate record retention for audit purposes.
- **Account Misuse:** Gaming accounts are intended solely for gaming activities. Deposits followed by negligible play and rapid withdrawals constitute misuse, trigger an immediate review, and may lead to suspension during the investigation.
- **Use of Multiple Accounts or Wallets:** The use of multiple accounts or wallets, even on separate Pelican Entertainment B.V. operated platforms, is considered suspicious. Internal monitoring systems identify linked accounts and flag them for comprehensive review and consolidation.
- **Third-Party Payments:** Where an account is funded with a payment method not in the customer's name, full KYC is required on both parties, along with evidence of their relationship and verification of fund legitimacy.
- **Criminal Proceeds:** Deposits may originate from illicit sources such as payment-card fraud, drug trafficking, or theft. Customers may need to provide proof of lawful source of funds, and any transactions suspected of involving criminal proceeds are reported to the Financial Intelligence Unit (FIU).

4.3 Geographic Risk Assessment

Pelican Entertainment B.V. employs a structured jurisdictional risk framework to evaluate risks associated with a customer's country of residence, location of activity, and the origin of their funds. The framework is continuously updated using authoritative international sources, including:

- Financial Action Task Force (FATF) public statements and high-risk jurisdiction lists
- The European Commission's list of high-risk third countries
- U.S. Office of Foreign Assets Control (OFAC) sanctions lists
- Advisories issued by the Caribbean Financial Action Task Force (CFATF)
- U.S. Department of State's International Narcotics Control Strategy Reports
- Transparency International's Corruption Perceptions Index

Prohibited Jurisdictions

The company does not accept customers located in or funding accounts from sanctioned jurisdictions under any circumstances. Jurisdictions subject to international sanctions for terrorism, weapons proliferation, or other criminal activities are generally prohibited. Exceptions, if considered, must be approved by senior management and comprehensive Enhanced Due Diligence (EDD).

High-Risk Jurisdictions

Enhanced Due Diligence (EDD) is mandatory for Clients from high-risk jurisdictions, including verification of source of funds and, where relevant, source of wealth. Establishing or maintaining the relationship requires senior management approval.

A jurisdiction is deemed high risk if any of the following conditions are present:

- Weak or deficient AML/CFT controls, or inadequate enforcement of such measures;
- Significant systemic corruption creating opportunities illegal financial flows;
- Connections to active terrorist organisations or jurisdictions flagged for supporting terrorist financing.

Enhanced Due Diligence measures:

- Obtaining complete documentation to verify the source of funds and, where applicable, the source of wealth;
- Performing robust, independent identity verification using reliable and authoritative data sources;
- Implementing ongoing enhanced transaction monitoring, focusing on unusual or complex activity;
- Conducting more frequent reviews of the customer profile and updating risk assessments on a regular basis;
- Requiring explicit senior management approval before establishing or continuing the business relationship.

Pelican Entertainment B.V. maintains accurate classifications by consulting authoritative sources including FATF's high-risk jurisdiction lists, the European Commission's AML/CFT deficiency lists, OFAC sanctions lists, CFATF statements, the U.S. Department of State's annual reports, and Transparency International's corruption indices, together with reports on countries supporting terrorist financing or harbouring terrorist groups.

If a customer's country of residence, citizenship, or fund origin is identified as high-risk or subject to international sanctions, the case must be escalated immediately to the Compliance Officer. Enhanced Due Diligence (EDD) measures must be applied, and the establishment or continuation of the business relationship requires senior management's approval.

Risk Factor	Description	Mitigation Plan
Weak AML/CFT Frameworks	Jurisdictions lacking robust AML/CFT controls or effective enforcement.	Require thorough SoF documentation and SoW where relevant; apply continuous enhanced monitoring.
High Levels of Corruption	Countries where corruption is widespread/systemic, increasing exposure to illicit funds.	Enhanced due diligence, prioritizing verification of declared income legitimacy.
International Sanctions	Jurisdictions subject to international sanctions for terrorism, proliferation financing, or other serious criminal activities.	Onboarding prohibited; no accounts may be opened or serviced.
Terrorist Activity	Jurisdictions linked to designated terrorist organizations or flagged for terrorist financing (TF) support.	Considered high risk by default. Require enhanced verification, continuous monitoring, and periodic risk re-evaluation.
Sanctioned Jurisdictions	Countries designated on sanctions registers maintained by the UN, EU, OFAC, or OFSI.	Onboarding prohibited; no accounts may be opened or serviced.

4.4 Channel and Technology Risks

Customer risk is closely tied to the access channel and underlying technology used to interact with Pelican Entertainment B.V. Differences in authentication methods, device integrity, and connection environments can materially alter exposure to financial crime. In this context, remote onboarding is a particular point of concern because it limits face-to-face verification and relies heavily on digital credentials, increasing exposure to impersonation, identity theft, and other forms of fraud.

To mitigate these risks, the company deploys an advanced digital KYC solutions. ore controls include biometric identity verification, automated document authenticity analysis, geolocation validation, liveness testing to prevent spoofing, and multi-factor authentication to secure account access.

The company does not introduce new technology or payment capabilities without first completing a pre-implementation risk assessment. This analysis evaluates whether the change could facilitate money laundering, fraud, sanctions evasion, or similar misconduct, and ensures preventive controls are built into the design and deployment plan.

Any channel that enables users to remain anonymous is designated high risk by default. Engagement through such channels triggers stricter requirements enhanced ID procedures, biometrics, and live sanctions/PEP checks. Although remote access is common across the sector, it remains high risk and is therefore supported by rigorous onboarding safeguards and continuous monitoring. To maintain protection beyond onboarding, secure identity validation is also applied during transactional activity to deter impersonation and account misuse.

Third-party facilitation of customer interactions introduces elevated risk, particularly when the intermediary falls outside AML/CFT oversight. Pelican Entertainment B.V. mitigates this by conducting comprehensive due diligence on both the intermediary and the customer, checking regulatory status, testing the sufficiency of AML/CFT controls, and validating data integrity. If the intermediary is unregulated or due diligence remains incomplete or unsatisfactory, the company will not proceed, or will exit any existing relationship, in compliance with AML rules.

Risk Factor	Description	Mitigation Plan
Remote Onboarding & Interaction	Remote (non-face-to-face) onboarding and transactions that elevate impersonation and identity-fraud risk.	Enforce robust digital safeguards: biometric validation, liveness detection, document verification, and multi-factor authentication.
Channels Enabling Anonymity	Methods that conceal or obscure user identity, reducing transparency and traceability.	Enforce strengthened identification and verification, including document authentication, biometric verification, and real-time screening against sanctions and PEP lists.
Third-Party Involvement	Customer interactions via intermediaries, with elevated risk if the intermediary is not AML/CFT supervised.	Conduct KYC/EDD on customer and intermediary, confirm intermediary regulatory standing and AML/CFT framework, ensure complete/accurate documentation, decline or end relationship if DD cannot be satisfied.

4.5 Risk Indicators

Pelican Entertainment B.V. evaluates each customer relationship through a structured set of risk indicators embedded in its Risk-Based Approach (RBA). These indicators covering factors such as geography, product/use case, channel, and customer profile are weighted to produce a risk score that places the relationship into clearly defined tiers. The resulting classification determines the depth of checks performed, ensuring that

standard due diligence or enhanced due diligence (EDD) is applied in proportion to the risk identified and revisited over the customer lifecycle.

A. Customer Profile Risk

Customer background and behaviour risk indicators include:

- Multiple, irregular, or non-transparent income sources
- Politically Exposed Person (PEP) status, or a close associate/family member of a PEP
- High, disproportionate, or unexplained spending patterns
- Sudden spikes in activity by casual or low-frequency players
- Use of third parties to fund or operate accounts
- Operation of multiple or linked accounts
- Redemption/withdrawal of funds without commensurate, verifiable gaming activity
- Association with junket operators or unregulated promoters

B. Product, Service, and Transaction Risk

Product and transaction behaviour indicators include:

- Evidence or suspicion that gaming activity is funded with illicit proceeds
- Payments funded through anonymous/semi-anonymous, or unregulated payment tools, including prepaid cards, e-wallets, or crypto
- Account misuse patterns (e.g., deposit → minimal play → withdrawal)
- Frequent changes in payment methods or instruments
- Account funded by third-party
- Identity fraud or attempts to use stolen credentials
- Use of multiple e-wallets or unlicensed financial service providers

C. Geographic Risk

Jurisdictions are considered high risk if they present:

- Inadequate or ineffective AML/CFT frameworks and/or lax enforcement
- Elevated corruption levels or systemic governance weaknesses
- Active sanctions for terrorism, proliferation financing, or other criminal activity
- Links to known terrorist organisations or financial crime networks
- Listed by international bodies, e.g. FATF, OFAC, the European Commission, CFATF, or Transparency International's Corruption Perceptions Index

D. Channel and Technology Risk

Indicators concerning how customers access services include:

- Use of channels that enable or attempt to preserve anonymity
- Remote onboarding conducted without robust identity verification and control checks
- Customer interactions mediated by unregulated or unverified third-party intermediaries

- Transactions processed through technologies or platforms lacking AML/CFT oversight

Risk Category	Common Red Flags	Required DD Measures
Customer Profile	Multiple or irregular income flows, PEP or familial/associate link, spending inconsistent with profile, pending inconsistent with profile, third-party funding/control, multiple or linked accounts, association with junket operators.	EDD required: verify/document income, perform SoW verification, require senior approval for PEPs, and conduct ongoing activity monitoring.
Products, Services & Transactions	Anonymous or unregulated payment channels (e.g., prepaid cards, certain e-wallets, cryptocurrencies), potential criminal-proceeds funding, misuse of accounts deposit → limited wagering → withdrawal), third-party funding reliance, identity-fraud attempts.	Perform enhanced verification of payment instruments, collect documentary proof of lawful SoF, apply monitoring rules to flag anomalies, escalate suspicions to the FIU.
Geographic	Links to countries lacking effective AML/CFT controls, elevated corruption levels, sanctions in force, or terrorism/proliferation finance exposure.	Screening against FATF, EU high-risk lists, OFAC, CFATF, and Transparency International CPI, apply stricter verification and EDD, escalate to the Compliance Officer, refuse or terminate relationships where links to sanctioned jurisdictions are identified.
Channels & Technology	Anonymity-enabling channels, remote onboarding with insufficient verification, third-party intermediaries lacking regulation/verification.	Implement advanced KYC: biometric and liveness detection, document authentication, geolocation, and multi-factor authentication, conduct full due diligence on third-party intermediaries, reject unverified/unregulated third parties.

Risk Scoring and Classification

Pelican Entertainment B.V. uses an internal Risk Calculator to ensure a consistent Risk-Based Approach. It scores each indicator, aggregates the results, and assigns customers to defined risk categories:

- **Low Risk:** Customers scored as low risk are subject to Standard Due Diligence. Documentation requirements are limited to statutory obligations or triggered by changes in the customer's profile.

- **Medium Risk:** Low and medium indicators present. Standard Due Diligence is applied with additional verification steps and closer, ongoing monitoring of activity.
- **High Risk:** Customers exhibiting any high-risk indicator are subject to mandatory Enhanced Due Diligence, including expanded identity and SoF/SoW verification, and senior management approval prior to onboarding. The relationship remains under heightened, risk-based monitoring for its duration, with a shortened review cycle and immediate escalation upon new adverse information.

This structured scoring framework delivers a uniform, risk-proportionate, evidence-based approach to customer due diligence. It also supports dynamic re-assessment, enabling rapid escalation when new or emerging risk signals appear.

Outcome of the Risk Assessment

The overall risk score determines the level of controls applied. Customers assessed as low risk are subject to standard customer due diligence and routine monitoring. Customers assessed as high risk must undergo enhanced due diligence, including approval by senior management before the relationship is established, along with ongoing, strengthened monitoring to detect and respond to suspicious activity throughout the relationship.

5. Onboarding Process

To safeguard the platform, Pelican Entertainment B.V. enforces a structured, compliance-driven onboarding framework to ensure that only customers who meet defined acceptance criteria can access the platform. Each application is assessed against documented standards, and any deficiencies must be resolved before proceeding. Accounts remain inactive until the customer has fully completed identity verification and sanctions screening.

Identification Requirements

During onboarding, every customer must provide complete identifying information, including full legal name, date and place of birth, nationality, residential address, and a unique identification number from an official document (e.g., passport or national identity card).

PEP and Sanctions Screening

All customers are screened against global sanctions lists and Politically Exposed Person (PEP) databases using automated systems to ensure full coverage. Any alerts or potential matches are then manually reviewed by compliance to verify accuracy and clear false positives. Screening is performed at onboarding and on an ongoing basis.

Enhanced Due Diligence for High-Risk Customers

When a customer is assessed as high risk, Pelican Entertainment B.V. initiates Enhanced Due Diligence (EDD). The customer must submit documentation confirming the legitimacy of funds and, where relevant, the source of wealth. This may take the form of recent bank statements, audited financial reports, tax documentation, property sale agreements, or statements of investments. The controls are mandated to satisfy AML/CFT requirements and reduce exposure to financial-crime risk.

6. Enhanced Due Diligence

Where elevated risk is present, Enhanced Due Diligence (EDD) is required. This group includes Politically Exposed Persons (PEPs) and their close associates and family members; customers connected to high-risk jurisdictions, who are nationals of, reside in, or fund accounts from high-risk countries; individuals engaging in unusually large or complex transactions, and clients with activity inconsistent with declared income/business. EDD typically requires enhanced documentation, third-party validation where feasible, approval at a senior level, and increased transaction monitoring.

Verification Measures and Controls

Enhanced Due Diligence (EDD) involves a deeper review than standard CDD. It requires a comprehensive assessment of the customer's source of funds and, where relevant, source of wealth, supported by independent, verifiable evidence. Further controls may involve consulting corporate registers and public records to verify beneficial owners, checking professional/business affiliations, reviewing audited financials, and conducting multi-source adverse-media and reputation assessments.

Approval and Oversight

High-risk customers can be onboarded only with senior management approval. In exceptionally complex or sensitive cases, formal authorisation from the Board of Directors may also be required.

Monitoring after Onboarding

Enhanced ongoing monitoring applies to all onboarded high-risk customers. This includes tighter thresholds for transaction reviews, closer scrutiny of activity, and more frequent reassessments of their risk profile, ensuring alignment with regulatory obligations and the company's risk appetite.

7. Ongoing Monitoring

Pelican Entertainment B.V. acknowledges that effective customer acceptance extends throughout the relationship. Continuous monitoring is used to confirm that behaviour remains aligned to the established risk profile and to surface any deviations promptly. Where anomalies arise, we initiate timely investigation, apply enhanced measures as needed, and document remediation or exit decisions.

Transaction Monitoring

Automated monitoring systems are used to detect anomalous or suspicious behaviour. Alerts may be generated for deposits or withdrawals that diverge from the customer's declared profile, rapid fund movement without commensurate gaming activity, use of multiple or atypical payment methods, or patterns indicative of collusion, chip-dumping, or other prohibited behaviour. Compliance officers review every alert, and determine whether escalation or further investigation is necessary.

Periodic Reviews and Risk Reassessment

In addition to real-time monitoring, Pelican Entertainment B.V. performs periodic, risk-based reviews of customer profiles to keep risk classifications current and accurate. Material changes, such as relocation to a high-risk jurisdiction, a marked rise in transaction volumes, or shifts in funding methods, prompt an immediate risk re-assessment. Where warranted, Enhanced Due Diligence (EDD) measures and tighter monitoring controls are applied.

8. Relationships Termination

Pelican Entertainment B.V. may suspend or terminate a customer relationship at its discretion, in accordance with AML/CFT obligations and internal standards. Termination may result from failure to provide required identification or supporting documentation within thirty (30) days, transactional behavior indicative of money laundering, terrorist or proliferation financing, or any breach of legal, regulatory, or Responsible Gambling Policy requirements.

Funds Handling and Reporting

When termination is linked to suspected criminal activity, Pelican Entertainment B.V. promptly files a report with the Financial Intelligence Unit (FIU) in accordance with the National Ordinance on the Reporting of Unusual Transactions (NORUT). Unless directed otherwise by law enforcement or regulatory authorities, customer funds are returned to the original funding source. Full documentation of the termination, including reasons and supporting materials, is retained for no less than five years.

Refusal or Termination

To comply with legal/regulatory requirements and internal risk policies, Pelican Entertainment B.V. may deny onboarding or terminate an existing customer relationship. The circumstances may include, but are not limited to, the following:

A. Failure to Meet Due Diligence Requirements

- a. The customer fails to provide required documents or information within the specified timeframe.
- b. False, misleading, or incomplete information provided during onboarding or verification.
- c. The customer is unable or unwilling to provide verifiable evidence of a legitimate source of funds (SoF) and, where applicable, source of wealth (SoW).

B. Jurisdictional and Legal Restrictions

- a. The customer's citizenship, residence, location, or transaction origination is tied to a sanctioned or prohibited jurisdiction.

C. Financial Crime & Regulatory Risks

- a. The customer is engaged in, or reasonably suspected of, money laundering, terrorist financing, proliferation financing, or other criminal activity.
- b. The customer is identified as a Politically Exposed Person (PEP), or a relative/close associate of a PEP, whose risk cannot be adequately mitigated.

D. Fraudulent or Prohibited Activity

- a. Participation in fraud, including but not limited to bonus abuse, collusive play, chip-dumping, or other manipulative use of the platform.
- b. Transactions routed through third parties without complete disclosure and verification.
- c. The customer requests significant withdrawals without matching, documented gaming activity.

E. Responsible Gambling & Player Protection

- a. The customer is subject to self-exclusion, or has been excluded under the company's Responsible Gambling Policy.

F. Age restrictions

- a. The customer is a minor or otherwise below the lawful gambling age where they reside.

9. Responsible Gambling Integration

Pelican Entertainment B.V.'s Customer Acceptance Policy is fully aligned with the Responsible Gambling framework. The prevention of gambling-related harm is embedded as a core obligation within the company's compliance and operations.

Indicators of Problem Gambling

Upon identifying signs of potential harm, such as deposits inconsistent with affordability or unusually extended periods of play, the company shall implement timely risk-mitigation measures, which may apply affordability/deposit limits, account suspension, or, where necessary, denying service to safeguard the customer.

Self-Exclusion and Account Restrictions

Self-exclusion requests are actioned immediately and applied across all accounts linked to the individual to ensure enforcement. The restrictions remain in force for the full term requested by the customer, or longer if mandated by regulatory requirements.

Employee Training and Compliance Awareness

Employees in customer-facing roles receive targeted training to recognise early indicators of gambling-related harm. This training is integrated into both initial onboarding and continuous monitoring processes to ensure timely intervention whenever risk factors are detected.

10. Record Keeping

Pelican Entertainment B.V., in line with AML/CFT and data-protection laws, retains customer-acceptance records for a minimum of five years after a business relationship ends. These records include KYC documentation, address verification, SoF/SoW evidence, monitoring alerts, EDD reviews, compliance findings, and termination files. All data is stored in encrypted systems with strict access controls. All data is stored in encrypted systems with strict access controls, monitored, and periodically reviewed to maintain accountability and regulatory compliance.

11. Policy Review and Approval

The Customer Acceptance Policy is reviewed at least once per year to ensure alignment with legislation, regulatory standards, and best practice. The review also considers shifts in the company's risk exposure, customer behaviour trends, and technological developments that may present new risks. Amendments are prepared by the Compliance Officer and escalated to the Board for approval.

Following approval, all changes are formally documented, communicated to relevant personnel, and integrated through training to guarantee consistent implementation.



(SMES) Solutions for Management and Employment Support N.V.
Managing Director
23.09.2025