
Director

HIGHFLIER B.V.

(Registration number 149996)

AML/CFT/CPF POLICY

Internal Procedure Rules and Internal Control Rules

Prevention of money laundering, terrorist financing and proliferation financing

Provider of B2B gambling services (supplier of gaming-related critical services and goods)

Jurisdiction: Curaçao

Version 2.0 | Effective date: 25.06.2026

Document Control

Item	Detail
Document title	AML/CFT/CPF Policy — Internal Procedure Rules and Internal Control Rules
Entity	HIGHFLIER B.V., registration number 149996
Business activity	Provider of B2B gambling services (gaming-related critical services and goods)
Version	2.0
Effective date	25.06.2026
Next review	At least annually, or upon a material change in law, risk or business

Contents

Document Control	2
Contents.....	3
1. Introduction and Purpose.....	4
2. Legal and Regulatory Framework	4
3. Scope and Application	5
4. Definitions	5
5. Governance and Responsibilities	6
6. Risk-Based Approach	7
7. Customer Acceptance Policy	8
8. Customer Due Diligence	8
9. Beneficial Ownership	9
10. Politically Exposed Persons	10
11. Sanctions Screening	10
12. High-Risk Countries	10
13. Ongoing Monitoring.....	11
14. Reporting Unusual Transactions to the FIU	11
15. Confidentiality and Prohibition of Tipping-Off.....	11
16. Record Keeping and Retention	12
17. Training and Awareness	12
18. Internal Controls and Independent Audit	12
19. Data Protection	12
20. Cooperation with Authorities	12
21. Review, Approval and Amendment.....	13

1. Introduction and Purpose

1.1 This policy sets out the internal procedure rules and internal control rules of HIGHFLIER B.V. (the Company) for the prevention of money laundering (ML), terrorist financing (TF) and proliferation financing (PF). It establishes how the Company identifies, assesses, manages and mitigates the ML/TF/PF risks arising from its activities as a provider of B2B gambling services in and from Curaçao.

1.2 The purpose of the policy is to protect the Company and the integrity of the Curaçao financial and gaming system from misuse, to comply with the obligations imposed on service providers and on suppliers in the gaming sector, and to support the Company's licensing position with the Curaçao Gaming Authority (CGA).

1.3 The policy is built on a risk-based approach. The Company applies measures that are proportionate to the nature, scale and complexity of its business and to the ML/TF/PF risks it faces.

2. Legal and Regulatory Framework

2.1 Curaçao is an autonomous country within the Kingdom of the Netherlands. It is not a Member State of the European Union or of the European Economic Area, and EU anti-money-laundering directives do not apply directly to it. The Company's obligations derive from Curaçao law and from the supervisory framework of the CGA, informed by the recommendations of the Financial Action Task Force (FATF) and the Caribbean Financial Action Task Force (CFATF).

2.2 The principal sources of obligation are:

- National Ordinance on Identification when Rendering Services (Landsverordening identificatie bij dienstverlening, LID / NOIS), as consolidated in PB 2017 no. 92 and as amended;
- National Ordinance on the Reporting of Unusual Transactions (Landsverordening melding ongebruikelijke transacties, LMOT / NORUT), as consolidated in PB 2017 no. 99 and as amended;
- the amending and consolidating AML/CFT/CPF legislation published in PB 2024 no. 41, including the National Ordinance on combating money laundering, the financing of terrorism and the financing of proliferation;
- the Sanctions National Ordinance (N.G. 2014 no. 55) and the Kingdom Sanctions Act (N.G. 2016 no. 54);
- the National Ordinance Financial Intelligence Unit (establishing the FIU as the national centre for receiving and analysing transaction reports);
- the PEP regulation (PEP-regeling, PB 2024 no. 126) and the regulation designating amounts, countries, states and documents for service providers (most recently PB 2026 no. 35);
- the National Ordinance on Games of Chance (Landsverordening op de kansspelen, LOK, PB 2024 no. 157), in force since 24 December 2024, which replaced the former offshore games regime and made the CGA the sole licensing and supervisory authority;

- the CGA Regulations for the combating of money laundering, the financing of terrorism and proliferation, and other CGA policies and guidelines issued under the LOK, the NOIS and the NORUT.

2.3 The CGA has been the AML/CFT supervisor for the gaming sector operating in and from Curaçao since 15 February 2019. As a holder of, or applicant for, a supplier (B2B) licence, the Company is required to comply with all CGA policies, procedures, regulations and guidelines relating to AML/CFT/CPF, and to make its records available to the CGA on request.

2.4 Where this policy refers to a monetary threshold, a list of high-risk countries, a reporting deadline or a procedural detail, the operative figure is the one set out in the applicable law, designation regulation or CGA regulation in force at the relevant time. The figures used in this policy are working references and must be kept current.

3. Scope and Application

3.1 This policy applies to the Company, to every member of its Management Board, to all employees, and to any agent or third party acting for the Company in a function relevant to AML/CFT/CPF.

3.2 The Company is a B2B supplier. Its customers are business counterparties, principally B2C gaming operators and other licensees, platform and payment counterparties, and other suppliers, rather than individual players. Customer due diligence under this policy is therefore directed primarily at legal entities, their ultimate beneficial owners (UBOs) and their controllers and key persons. The Company does not maintain player accounts and does not directly onboard players.

3.3 Because the Company's services can be used by operators who deal directly with players, the Company takes reasonable steps to satisfy itself that its operator clients are appropriately licensed and that they themselves maintain AML/CFT/CPF controls. The Company does not provide services to operators it knows or suspects to be unlicensed where a licence is required, or to operators that refuse to provide the information needed for due diligence.

3.4 The policy applies to the establishment of every business relationship, to occasional transactions, and to the ongoing conduct of relationships, including where activity is conducted through agents or where activities are outsourced to a third party.

4. Definitions

Term	Meaning
Money laundering (ML)	Conversion, transfer, concealment, acquisition, possession or use of property known to derive from criminal activity, and participation in or facilitation of such acts. Property is treated as criminally derived regardless of where the predicate offence took place and even where the predicate offence has not been separately identified.
Terrorist financing (TF)	The provision or collection of funds or other property with the intention or knowledge that they are to be used to carry out terrorism, as defined in the Penal Code of Curaçao.

Proliferation financing (PF)	The provision of funds or financial services used for the manufacture, acquisition or transport of weapons of mass destruction, in breach of applicable sanctions and prohibitions.
Customer / client	A business counterparty that has, or seeks to establish, a business relationship with the Company, together with any person participating in an occasional transaction with the Company.
Beneficial owner (UBO)	The natural person who ultimately owns or controls the customer, through direct or indirect ownership of a sufficient percentage of shares, voting rights or ownership interest, or through control by other means, or on whose behalf a transaction is conducted.
Politically exposed person (PEP)	A natural person who is or has been entrusted with a prominent public function, together with that person's family members and known close associates, as further defined in the PEP regulation.
Unusual transaction	A transaction that meets an objective indicator set by law or regulation, or that gives rise, on subjective grounds, to a suspicion that it may relate to ML, TF or PF. Curaçao operates an unusual-transaction reporting regime rather than a suspicious-transaction regime.
FIU	The Financial Intelligence Unit of Curaçao, the national body that receives, requests, analyses and disseminates unusual transaction reports.
CGA	The Curaçao Gaming Authority, the licensing authority and AML/CFT supervisor for the gaming sector under the LOK.
goAML	The electronic reporting system used to submit unusual transaction reports to the FIU.
BRA / CRA / CAP	Business Risk Assessment, Customer Risk Assessment and Customer Acceptance Policy.

5. Governance and Responsibilities

5.1 Management Board

The Management Board owns this policy and is responsible for compliance with the AML/CFT/CPF framework. The Board approves the policy and the risk assessments, allocates sufficient resources to the compliance function, approves the establishment or continuation of higher-risk relationships where this policy requires it, and ensures that staff are trained. Each Board member confirms by signature that they have read and understood this policy. The Board reviews the policy at least once a year and whenever the law, the Company's risk profile or its business changes materially.

5.2 Responsible Management Board member

Where the Company has more than one Board member, the Board appoints one member to be responsible for the implementation of the AML/CFT/CPF framework and for liaison with the CGA and the FIU.

5.3 Compliance Officer

The Company appoints a Compliance Officer who is responsible for the day-to-day operation of the AML/CFT/CPF programme. The Compliance Officer designs and maintains the controls, performs and documents the risk assessments, conducts and reviews customer due diligence, monitors transactions and business activity, decides on and submits unusual transaction reports to the FIU, maintains records, organises training and reports periodically to the Management Board.

The Compliance Officer must be fit and proper and must meet the CGA suitability requirements. In particular, the role is independent of operational functions and is not combined with the role of CEO, CFO, COO, UBO or internal auditor. The Compliance Officer must have appropriate knowledge of the NOIS and the NORUT, of applicable EU and OFAC sanctions, and of the CGA regulations, hold a recognised AML qualification where required (for example CAMS or AMLFC), and complete the required annual AML training (at least 10 hours).

The compliance function may be outsourced to a qualified provider, but the Company retains ultimate responsibility. The contact details of the Compliance Officer are recorded in Annex A.

5.4 Staff obligations

Every employee must know and follow this policy, recognise indicators of ML, TF and PF, escalate concerns to the Compliance Officer without delay, and refrain from acting where due diligence cannot be completed. Failure to comply may lead to disciplinary action and termination of employment, without prejudice to any legal consequences.

6. Risk-Based Approach

6.1 Business Risk Assessment (BRA)

The Company prepares and documents a Business Risk Assessment that identifies and assesses the ML/TF/PF risks inherent in its business. The BRA covers at least the following categories of risk:

- customer risk, including the type, ownership and licensing status of operator clients;
- country and geographic risk, including the jurisdictions of clients, their UBOs and their players;
- product, service and transaction risk, including the gaming-related services and goods the Company supplies;
- delivery channel and technology risk, including remote onboarding, new or developing technologies and the use of virtual assets.

The BRA is reviewed at least annually and whenever a material change occurs, for example before launching a new product, service, delivery channel or technology. The BRA is approved by the Management Board and made available to the CGA on request.

6.2 Customer Risk Assessment (CRA)

For each customer the Company performs a Customer Risk Assessment and assigns a risk rating of low, medium or high. The rating drives the level of due diligence applied and the intensity of

ongoing monitoring. The CRA takes account of the customer's ownership and control structure, its licensing status and regulatory history, the jurisdictions involved, the nature and volume of the expected relationship, and any PEP or sanctions exposure.

6.3 Risk appetite

The Management Board sets the Company's risk appetite in writing. The risk appetite states the customer characteristics and circumstances the Company will avoid, those that require enhanced due diligence, and the conditions under which a relationship will be refused or terminated.

7. Customer Acceptance Policy

7.1 The Company will not establish or maintain a business relationship, and will not carry out an occasional transaction, where:

- the customer or its UBO cannot be identified and verified;
- the customer refuses to provide the information or documents required for due diligence, or provides information that is false or cannot be verified;
- the customer, its UBO or a controller appears on an applicable sanctions list;
- the Company knows or suspects that the relationship would facilitate ML, TF or PF;
- the customer is an operator that requires a gaming licence and does not hold a valid one, or relies on an authority that is no longer valid;
- the person acting cannot be shown to be acting on their own behalf, and the person on whose behalf they act cannot be identified.

7.2 The Company does not keep anonymous accounts or accounts in obviously fictitious names. Where acceptance is refused or a relationship is terminated for AML/CFT/CPF reasons, the Compliance Officer records the circumstances and considers whether an unusual transaction report is required.

8. Customer Due Diligence

8.1 When CDD is applied

The Company applies customer due diligence before establishing a business relationship, before carrying out an occasional transaction at or above the applicable threshold, when there is a suspicion of ML, TF or PF regardless of any threshold, and when there is doubt about previously obtained identification data. Verification is completed before binding measures are taken; where verification is completed during onboarding so as not to disrupt the ordinary course of business, it is carried out as quickly as possible and the relationship is restricted until it is complete.

8.2 Standard CDD for legal-entity customers

For a corporate customer the Company identifies and verifies at least the following, using documents and information from reliable and independent sources:

- the legal name, legal form, registration number, registered and operating addresses, and date of incorporation;

- an extract from the commercial register and the constitutional documents;
- the ownership and control structure, and the identity of each UBO, verified to the Company's satisfaction;
- the identity and authority of the representatives acting for the customer;
- the licensing status of the customer where it operates in a regulated activity, including its CGA or other gaming licence where applicable;
- the purpose and intended nature of the business relationship, the expected activity and volumes, the main counterparties and the source of funds and, where relevant, source of wealth.

The customer confirms the accuracy of the information provided. The Company may accept certified or notarised copies, and documents executed abroad must be legalised or apostilled where required. Electronic identification and verification from at least two independent reliable sources may be used where the original document cannot be inspected.

8.3 Simplified due diligence

Simplified due diligence may be applied only where the BRA and the CRA establish that the relationship presents a genuinely lower risk, and only to the extent that the Company can still monitor the relationship and detect unusual transactions. Simplified due diligence reduces the intensity of measures; it never removes the obligation to identify and verify the customer and its UBO, to screen for sanctions and PEP status, or to report unusual transactions.

8.4 Enhanced due diligence (EDD)

The Company applies enhanced due diligence to higher-risk relationships. EDD is always applied where:

- there is doubt about the truthfulness of information, the authenticity of documents or the identity of the UBO;
- the customer, its UBO or a controller is a PEP, a family member or a known close associate of a PEP (other than as limited by the PEP regulation for local PEPs);
- the customer, its UBO, or the relevant payment service provider is based in a high-risk third country or in a jurisdiction with weak AML/CFT controls or under relevant sanctions;
- the BRA or CRA identifies a higher-than-usual risk for the activity, product or channel.

EDD measures include obtaining additional identifying information and documents, establishing the source of funds and source of wealth, obtaining senior management approval to establish or continue the relationship, verifying the rationale and substance of transactions to rule out sham arrangements, and applying more frequent and more intensive monitoring. For higher-risk relationships the Company reassesses the customer's risk profile at least every six months.

9. Beneficial Ownership

9.1 The Company identifies the UBO of every legal-entity customer and takes reasonable measures to verify the UBO's identity so that it is satisfied it knows who the UBO is and

understands the ownership and control structure. The Company records the steps taken to identify the UBO.

9.2 Where a customer is unwilling or unable to disclose its UBO, or where the structure is opaque without a credible explanation, the Company does not proceed and considers whether a report to the FIU is required.

9.3 Where a natural person appears to be acting under the control of, or on behalf of, another person, the Company identifies that other person and treats the relationship accordingly.

10. Politically Exposed Persons

10.1 The Company establishes whether a customer, its UBO or a controller is a PEP, a family member of a PEP or a known close associate of a PEP, using its own enquiries and reputable screening sources. Screening is performed at onboarding and is repeated during the relationship.

10.2 Establishing or continuing a relationship that involves a PEP requires the approval of senior management. The Company establishes the source of wealth and source of funds of the PEP and applies enhanced ongoing monitoring.

10.3 Where a person ceases to hold a prominent public function, the Company continues to apply a risk-based approach for at least the period required by the PEP regulation, until it is satisfied that the PEP-related risk no longer arises.

10.4 The PEP regulation (PB 2024 no. 126) governs the definitions and the precise treatment of domestic and foreign PEPs and of former PEPs. The Company maintains a current screening procedure and records the checks performed.

11. Sanctions Screening

11.1 The Company screens every customer, UBO, controller and, where relevant, counterparty against the sanctions lists applicable under the Sanctions National Ordinance and the Kingdom Sanctions Act, and against the United Nations, European Union and OFAC lists used in practice. Screening is performed at onboarding, before relevant transactions and on an ongoing basis, including when lists are updated.

11.2 Where a match is identified or reasonably suspected, the Company does not proceed with the relationship or transaction, freezes any assets as required, and reports without delay to the FIU and to any other competent authority. The Compliance Officer documents the match and the action taken.

12. High-Risk Countries

12.1 The Company maintains and keeps current a list of high-risk countries. The list is dynamic and is built from the FATF lists of high-risk and monitored jurisdictions, the countries designated in the applicable Curaçao designation regulation, jurisdictions under relevant sanctions, and other credible indicators of weak AML/CFT controls, significant corruption or terrorist activity. The Company does not rely on a fixed list embedded in this policy.

12.2 Where a customer, its UBO or the relevant payment service provider is connected to a high-risk country, the Company applies enhanced due diligence, including additional information on the customer and UBO, on the purpose and background of transactions, and on the source of funds and wealth, senior management approval, and intensified monitoring.

13. Ongoing Monitoring

13.1 The Company monitors each business relationship so that activity remains consistent with its knowledge of the customer and the customer's risk profile. Monitoring includes keeping due diligence information current, paying particular attention to complex, unusually large or unusual patterns of activity with no apparent economic or lawful purpose, and identifying the source and origin of funds where relevant.

13.2 Monitoring is intensified for higher-risk relationships and for relationships connected to high-risk countries. The frequency and depth of monitoring follow the risk rating assigned in the CRA.

14. Reporting Unusual Transactions to the FIU

14.1 Curaçao operates an unusual-transaction reporting regime under the NORUT. Objective indicators set by law and regulation, and subjective indicators based on suspicion, determine whether a transaction must be reported. By way of working reference, a transaction in the gaming context at or above the designated amount (for example NAf 5,000, to be confirmed against the current designation regulation) is reportable on objective grounds, and any transaction giving rise to a suspicion of ML, TF or PF is reportable on subjective grounds regardless of amount.

14.2 The Company reports an unusual transaction to the FIU without delay and within the period required by law. Reports are submitted electronically through the goAML system, together with the identification data and any supporting documents. The Compliance Officer is responsible for deciding on and submitting reports and for responding to FIU enquiries promptly and completely.

14.3 Where a transaction must be reported, the Company postpones it until the report is submitted, unless postponement is impossible, would cause disproportionate harm or would hinder the investigation, in which case the transaction is carried out and the report is submitted immediately afterwards.

14.4 Every employee must inform the Compliance Officer of any refusal to establish a relationship on AML/CFT grounds, of any suspicion of ML, TF or PF, and of any unusual transaction.

15. Confidentiality and Prohibition of Tipping-Off

15.1 The Company, its Board members and its employees must not inform a customer, its UBO, its representative or any third party that a report has been or will be made to the FIU, or that an investigation is taking place. Information about a report may be shared only with the FIU, with an authority conducting a related criminal investigation, and with a court acting under a court order.

15.2 Breach of the prohibition on tipping-off is a serious matter and may carry criminal consequences.

16. Record Keeping and Retention

16.1 The Company retains the documents and data used to identify and verify customers and UBOs, the documents underlying each business relationship, the correspondence relating to AML/CFT/CPF duties, the records of monitoring, and the data underlying unusual transaction reports.

16.2 Records are retained for at least five years after the end of the business relationship or after the relevant transaction, or for longer where required by law or by the FIU or CGA. Records are kept securely and in a form that allows the Company to respond fully and promptly to enquiries from the FIU, the CGA, investigative bodies and the courts.

17. Training and Awareness

17.1 All relevant staff and Board members receive AML/CFT/CPF training on appointment and at least once a year. Training covers this policy, the legal framework, current methods of ML, TF and PF, the recognition of unusual transactions, the reporting procedure, data protection and the consequences of non-compliance.

17.2 The Compliance Officer keeps records of the training delivered and of attendance, and updates training to reflect changes in law, in supervisory expectations and in the Company's risk profile.

18. Internal Controls and Independent Audit

18.1 The Company maintains an internal control system under which the work of staff is supervised by the Compliance Officer and the responsible Board member, and under which the Compliance Officer reports to the Management Board at least quarterly.

18.2 The effectiveness of the AML/CFT/CPF programme is tested by an independent audit. The Company arranges an independent audit by a qualified party on at least an annual basis, and provides the audit report to the CGA where required. Findings are tracked to remediation by the Management Board.

18.3 The Management Board ensures that adequate resources are allocated to the compliance function and that only suitably trained staff perform AML/CFT/CPF tasks.

19. Data Protection

19.1 The Company processes personal data gathered for AML/CFT/CPF purposes only for those purposes and does not use it for unrelated purposes such as marketing. The Company applies appropriate security measures and informs customers, before the relationship begins, of the processing carried out for AML/CFT/CPF purposes.

20. Cooperation with Authorities

20.1 The Company cooperates with the FIU, the CGA and other competent and law-enforcement authorities. It responds to lawful requests within a reasonable time, provides the information at its disposal, and observes the restrictions and confidentiality requirements set out in law.

21. Review, Approval and Amendment

21.1 The Management Board reviews and, where necessary, updates this policy at least once a year and whenever the law, the supervisory framework, the Company's risk profile or its business changes materially. Amendments take effect on approval by the Board.

21.2 This policy supersedes all previous internal procedure rules and internal control rules of the Company on the prevention of ML, TF and PF.



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

Managing Director

25.06.2026