ANTI-MONEY LAUNDERING, COUNTERING FINANCING OF TERRORISM AND COUNTERING FINANCING OF PROLIFERATION POLICY

Deep Dive B.V.

Subject	Anti-Money Laundering, Countering Financing of Terrorism and Countering Financing of Proliferation of Weapons of Mass Destruction Policy (AML/CFT/CFP Policy)
Purpose	Deep Dive B.V. policy document containing policies to comply with AML/CFT/CFP legislative and regulatory requirements, including the CGA Regulations effective 9 January 2025.
Version	1.2
Involvements	All departments
Responsibility	Money Laundering Reporting Officer (MLRO)
Approval	Board of Directors
Review	Annually or earlier as needed
Classification	Company Confidential — General | Including External

I hereby certify that this document is a true copy of the original document, which I have seen and verified in its original form.

Darryl Cassar
18A, Ferdinand Court, P/H 7,
Triq Lapsi, Sigglewi, SGW1968, Malta
+356 79286034
Certified Public Accountant
Warrant No: 12155

28/5/26

Change History

Date	Ver.	Author	Summary of Changes	MLRO
19/08/2024	1.0	Deep Dive B.V.	New document created as part of the AML/CFT Program review.	M. Taylor
30/05/2025	1.1	Deep Dive B.V.	Updated in line with Curaçao AML/CFT Policy guidelines.	M. Taylor

Date	Ver.	Author	Summary of Changes	MLRO
20/05/2025	1.2	Deep Dive B.V.	Comprehensive revision to align with CGA Regulations for ML/FT/CFP effective 9 January 2025 (enforcement from 10 April 2025). Added: Financing of Proliferation (CFP) as third pillar; Technological Developments Risk Assessment; Beneficial Owner identification; CDD timing rules; SDD framework; expanded EDD and PEP categories; Targeted Financial Sanctions freeze procedure; goAML reporting; Independent Audit function; Anonymous account prohibition; NRA reference; corrected transaction threshold to NAf 4,000 throughout; updated regulatory framework references.	V. Pirnau

1. Introduction

"Money laundering" is generally defined as engaging in acts designed to conceal or disguise the nature, control, or true origin of criminally derived proceeds so that those proceeds appear to have been derived from legitimate activities or otherwise constitute legitimate assets. Money Laundering consists of three phases: Placement (introducing illegal proceeds into the financial system), Layering (converting proceeds to disguise the audit trail), and Integration (re-entry of funds into the economy as apparently legitimate transactions).

"Financing of Terrorism" (FT) is the financing of terrorist acts, terrorists, and terrorist organisations. Unlike money laundering, the funds used to finance terrorism are not necessarily derived from illicit proceeds — FT is primarily concerned with obscuring the end recipient of funds rather than the source.

"Financing of Proliferation" (FP) is the provision of funds for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling, or use of nuclear, chemical or biological weapons and their means of delivery and related materials.

The Proceeds of Crime are funds derived from illicit sources from which a benefit or enjoyment may be obtained. Although the aim may not be to launder funds or to fund terrorism or proliferation, such activity is still illegal and subject persons must report it as if it were ML/FT/FP.

The policies set forth herein (the "Policies") are intended to satisfy the statutory requirements of the relevant legislation and to provide direction to Deep Dive B.V. (the "Company") in complying with its obligations at law by taking all reasonable steps and exercising all due diligence to avoid the commission of an offence of money laundering, funding of terrorism, or financing of proliferation of weapons of mass destruction.

The Company is aware that criminals, terrorists, and proliferators may attempt to use its services to channel funds from illegal activities. The National Ordinance on the Reporting of Unusual Transactions (NORUT) provides indicators to help identify unusual transactions. These indicators (consisting of objective and subjective indicators) describe when an executed or intended transaction is to be labelled as unusual and must be reported to the pertinent national authorities.

Objective Indicators — the reporting entity is obliged to report:

- A transaction reported to the police or judicial authorities in connection with money laundering or the financing of terrorism or proliferation.
- An intended transaction carried out by or for the benefit of a person, legal person, group or entity mentioned on a sanctions list compiled pursuant to the Sanctions National Ordinance.
- A transaction giving cause to assume it may relate to money laundering, terrorist financing, or financing of proliferation.
- A transaction amounting to NAf 4,000 or more, regardless of whether carried out in cash, via cheque or other payment instrument, electronically or in any other non-physical manner. This includes:
  - A giro-based transaction (bank-to-bank transfer) of NAf 4,000 or more.
  - Taking into or releasing from deposit an amount of NAf 4,000 or more at the client's request.
  - Sale of tokens/chips/credits to a client in the amount of NAf 4,000 or more.
  - Payout of prizes in the amount of NAf 4,000 or more.
  - All other cases meeting or exceeding NAf 4,000.

Subjective Indicators — the reporting entity has a reporting obligation where:

Based on knowledge of the client, their income and business activities, their gaming-related activity, and any other relevant circumstances, the reporting entity has reasonable grounds to presume that a transaction is related to money laundering, terrorism financing, or financing of proliferation.

2. Regulatory Framework

The following legislation and regulations are applicable to the Company's AML/CFT/CFP obligations:

- CGA Regulations for Combating Money Laundering, the Financing of Terrorism and Proliferation of Weapons of Mass Destruction — effective 9 January 2025, enforcement from 10 April 2025.
- National Ordinance on Identification when Rendering Services (NOIS) (N.G. 2017, no. 92).
- National Ordinance on the Reporting of Unusual Transactions (NORUT) (N.G. 2017, no. 99).
- Ministerial Decree with general operation of 11 November 2015, laying down the indicators as mentioned in Article 10 of the NORUT (Regulation Indicators Unusual Transactions) (N.G. 2015, no. 73).
- National Decree on rules for reporting unusual transactions (goAML portal) (Landsbesluit goAML meldportaal).
- Sanctions National Ordinance (N.G. 2014, no. 55).
- Kingdom Sanction Act (N.G. 2016, no. 54).
- National Decree entering into force of Kingdom Sanction Law (N.G. 2017, no. 2).
- National Decree of 10 July 2015 — implementation of Council Resolutions concerning Al-Qaeda, Taliban, ISIL, ANF and locally designated persons and organisations (N.G. 2015, no. 29).
- National Decree of 10 July 2015 — Sanctions Ordinance Libya (N.G. 2015, no. 28).
- National Decree — Sanctions National Ordinance extension of validity sanction decrees 2018 (N.G. 2018, no. 34).
- National Ordinance on Games of Chance (LOK).
- The Code of Criminal Law (Penal Code) (N.G. 2011, no. 48).

The Company shall also have regard to the outcomes and recommendations of the Curaçao National Risk Assessment (NRA) and relevant guidance published from time to time by the Curaçao Gaming Authority (CGA), the Financial Action Task Force (FATF), and the Caribbean Financial Action Task Force (CFATF).

3. Scope of this Policy

This Policy establishes the minimum standards from which procedures on internal control, risk assessment, risk management, and compliance in relation to AML/CFT/CFP are drawn up. It applies to all directors, officers, employees, agents, and sub-contractors of Deep Dive B.V.

The Company is determined and committed to preventing the use of its systems for activities related to money laundering, financing of terrorism, and financing of proliferation of weapons of mass destruction (ML/FT/FP). The Company shall comply with its obligations by establishing the necessary processes to prevent ML/FT/FP and to ensure that any suspicious activity is escalated to the relevant authorities without delay.

This Policy outlines general and minimum standards of internal AML/CFT/CFP controls which must be adhered to by the Company's management and all employees. Specific operational procedures implementing this Policy are documented separately and must be read in conjunction with this Policy.

The Company expressly prohibits the maintenance of anonymous accounts or accounts held in obviously fictitious names. Every customer must be identified and their identity verified before or during the establishment of a business relationship, in accordance with the CDD requirements set out in Section 8.

4. Money Laundering Reporting Officer

A Money Laundering Reporting Officer (MLRO) is appointed to be the business owner of the Company's AML/CFT/CFP Risk Assessment, Controls, Policies, and Procedures. The MLRO must be operationally independent of business functions and shall report directly to the Board of Directors without impediment. The MLRO must have unrestricted access to all customer data, transaction records, and other information necessary to discharge their duties.

The MLRO's responsibilities include, but are not limited to:

- Risk assessment and risk management, including maintenance of the Business Risk Assessment (BRA) and Customer Risk Assessment framework.
- Ensuring Customer Due Diligence (CDD) measures and ongoing monitoring are properly implemented.
- Record-keeping in accordance with legislative requirements.
- Promoting internal control and a culture of AML/CFT/CFP compliance.
- Overseeing the AML/CFT/CFP Compliance Programme (see Section 12).
- Monitoring and managing compliance with, and internal communication of, all AML/CFT/CFP policies and procedures.
- Monitoring of relevant staff and agent screening.
- Self-education and education of relevant staff in AML/CFT/CFP on an annual basis, or more regularly if deemed necessary.
- Liaison with law enforcement authorities and the Financial Intelligence Unit (FIU).
- Managing Investigation Order requests received from the authorities.
- Filing Unusual Transaction Reports (UTRs) via the goAML platform (see Section 13).
- Ensuring the independent audit function reviews the AML programme at least annually and reporting findings to the Board.

Note: *The MLRO shall not perform the independent audit of their own programme. An independent auditor — either from an internal audit function or an external third party — must carry out the annual review of the AML/CFT/CFP programme (see Section 12.5).*

5. Risk Assessment

5.1 Business Risk Assessment (BRA)

The Company must conduct and maintain a Business Risk Assessment (BRA) to identify the ML/FT/FP risks to which it is exposed and to ensure that policies, controls, and procedures are adequate to prevent and mitigate those risks. The BRA must be documented, approved by the Board of Directors, and made available to the CGA upon request.

The BRA must address the following four risk areas:

- Customer Risk — the risk posed by different types of players and business relationships.
- Geographical Risk — the risk arising from the nationality, residence, and country of origin of players and payment methods.
- Product, Service and Transaction Risk — the risk inherent in the products and services offered and the payment methods accepted.
- Distribution Channel Risk — the risk arising from the channels through which business relationships are established and transactions executed.

The BRA documentation must include:

- The methodology adopted for the assessment.
- The reasons for rating each risk factor as low, medium, or high risk.
- The outcome of the BRA, including the Company's risk appetite (i.e. the level of residual ML/FT/FP risk the Company is prepared to accept).
- The information sources used, including the outcomes and recommendations of the Curaçao National Risk Assessment (NRA) and guidance from FATF and CFATF.
- Measures implemented to mitigate identified risks.

The BRA must be reviewed at least once annually or whenever a significant change occurs — such as introduction of a new product, a new payment method, entry into a new market, or a change in the regulatory environment. The Board of Directors and MLRO must approve all versions of the BRA.

5.2 Risk Appetite Statement

Once the Business Risk Assessment is complete, the Board of Directors shall set and approve a Risk Appetite Statement defining the level of ML/FT/FP risk the Company is prepared to accept. The risk appetite informs Customer Due Diligence thresholds, the Customer Acceptance Policy, and the circumstances under which business will be declined. The Risk Appetite Statement is reviewed annually alongside the BRA.

5.3 Customer ML/FT/FP Risk Assessment

Each customer must undergo a Customer Risk Assessment (CRA) prior to establishing a business relationship or carrying out an occasional transaction. The CRA must be revised throughout the business relationship whenever there is a material change in the customer's profile or activity. The CRA enables the Company to categorise each customer's ML/FT/FP risk as low, medium, or high, and to apply the appropriate level of Customer Due Diligence (CDD).

Customer risk factors include, but are not limited to:

- Customer type and source of income/wealth.
- Products used (e.g. sportsbook, casino, poker, bingo).
- Transaction patterns and payment methods used.
- Delivery and distribution channels.

DC

- Geographical origin of the customer, their nationality, country of birth, and country of residence.
- PEP status and sanctions screening result.
- Whether the customer is a high spender relative to apparent income.
- Unusual deposit/withdrawal patterns such as depositing and immediately withdrawing with minimal or no play.

After registration, a customer's activity undergoes ongoing monitoring through automated and manual processes to detect changes in risk profile and to establish when due diligence thresholds have been reached.

5.4 Technological Developments Risk Assessment

Prior to launching any new product, business practice, delivery mechanism, or technology (including new or developing technologies applied to existing products), the Company must conduct and document a specific risk assessment to determine whether the innovation creates a vulnerability that could be exploited for ML/FT/FP purposes.

Where risks are identified through the technological developments assessment, proportionate mitigation measures must be designed and implemented before the product or technology is launched. The MLRO must approve the assessment and any associated mitigation plan.

6. Politically Exposed Persons and Sanctions

6.1 Politically Exposed Persons (PEPs)

A Politically Exposed Person (PEP) is a natural person who is or has been entrusted with a prominent public function. The Company distinguishes between the following categories, each carrying distinct obligations:

(a) Foreign PEPs

Individuals who are or have been entrusted with prominent public functions by a foreign country (e.g. heads of state or government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, and important political party officials). Foreign PEPs must always be treated as high-risk, regardless of other factors. Enhanced Due Diligence must be applied, and the business relationship must be approved by senior management.

(b) Domestic PEPs

Individuals who are or have been entrusted with prominent public functions within Curaçao or the Dutch Kingdom. Domestic PEPs are subject to a risk-based assessment. Where the risk assessment indicates a higher-than-average risk, EDD must be applied and senior management approval obtained.

(c) International Organisation PEPs

Persons entrusted with prominent functions by an international organisation (e.g. senior management of international bodies such as the UN, IMF, or World Bank). These customers must be subject to a risk-based assessment and, where appropriate, EDD.

(d) Relatives and Close Associates (RCAs)

Family members (spouses, partners, children and their spouses/partners, and parents) and known close associates of any PEP. RCAs are to be treated with the same level of caution as the PEP to whom they are connected.

Customers are asked on first deposit to confirm whether they are a PEP or a relative or close associate of a PEP. PEP screening is also carried out when a customer's risk profile moves above low risk or when relevant thresholds are reached. PEP checks are carried out using Shufti PRO software. Sanctioned individuals and persons connected to sanctioned entities cannot be accepted as customers.

6.2 Sanctions Screening

The Company screens all customers against the following sanctions and high-risk lists before the first deposit is initiated. Re-screening is carried out on a risk-sensitive basis and whenever triggered by changes to the customer's profile:

- United Nations Security Council Consolidated Sanctions List.
- European Union Consolidated Sanctions List.
- USA — Office of Foreign Assets Control (OFAC) Specially Designated Nationals (SDN) List.
- Curaçao National Sanctions Lists (when applicable).
- FATF High-Risk Jurisdictions subject to a Call for Action.
- FATF Jurisdictions under Increased Monitoring.
- CFATF Public Statement jurisdictions.
- US Department of State International Narcotics Control Strategy Report (INCSR).
- Basel AML Index.
- Transparency International Corruption Perceptions Index.

- Local sanctions lists for all jurisdictions where the Company operates or from which players are accepted.

The Company monitors the GCB website regularly for amendments to Sanctions Decrees and Regulations and updates its CDD and AML/CFT/CFP policies and procedures accordingly.

6.3 Targeted Financial Sanctions — Asset Freezing Procedure

Compliance with targeted financial sanctions is mandatory under the Charter of the United Nations and the Kingdom Sanctions Act. Upon identifying that a customer is or becomes a sanctioned person or entity, the Company shall act immediately and without prior notice as follows:

- Immediately freeze all funds held in the customer's account(s), preventing any withdrawal, transfer, or access to funds.
- Ensure that no further deposits, credits, or payments are made available to the sanctioned person or entity.
- File a report with the FIU Curaçao via the goAML platform without delay.
- Notify the MLRO and the Board of Directors immediately.
- Record all actions taken, the time of each action, and the basis for the freeze decision.
- Follow the Process for the Freezing of Resources (Proces bevriezing van middelen) as published in the National Gazette on 16 September 2016.

At minimum, a mechanism must exist to check the sanctions status of a customer at the point of any withdrawal request, so that a sanctioned person or organisation cannot remove money from an account that should be frozen. The Company shall not unfreeze assets without explicit authorisation from the competent authority.

7. Customer Acceptance Policy

The Company maintains a Customer Acceptance Policy (CAP) which sets out:

- A description of the types of customers likely to pose a higher-than-average risk of ML/FT/FP.
- The risk indicators presenting low, medium, or high risk.
- The level of CDD measures, including ongoing monitoring, to be applied at each risk tier.
- The circumstances under which service to a customer will be declined or an existing relationship terminated.
- PEP and Sanctions Screening requirements and procedures.

The Company will decline to establish or will terminate a business relationship where:

- The customer fails to complete the required CDD within the specified timeframe.
- The customer is identified as a sanctioned individual or entity.
- The customer is resident in or their funds originate from a high-risk jurisdiction from which the Company does not accept customers.
- There is an unacceptable risk of ML/FT/FP that cannot be mitigated by enhanced measures.
- The customer provides false, misleading, or unverifiable identification information.

8. Customer Due Diligence

8.1 Overview

Customer Due Diligence (CDD) is the process by which the Company identifies its customers, verifies that they are who they claim to be, understands the purpose of the business relationship, and monitors the relationship on an ongoing basis. A sound CDD programme is the primary defence against the Company being used for ML/FT/FP.

CDD measures must be applied:

- When players engage in financial transactions equal to or above NAf 4,000.
- When carrying out occasional transactions above the monetary equivalent of NAf 4,000.
- When a series of linked transactions, individually below NAf 4,000 but cumulatively meeting or exceeding NAf 4,000, is identified.
- When there is a suspicion of money laundering, financing of terrorism, or financing of proliferation.
- When the Company has doubts about the veracity or adequacy of previously obtained customer identification data.

8.2 Standard CDD Measures

The mandatory CDD measures are:

(a) Identification and Verification of the Customer

The Company must collect identifying details of the customer and verify their identity using reliable, independent source documents, data, or information. The extent of verification varies with the customer's risk rating. Identification details include at minimum: full name, date of birth, nationality, address, and a government-issued photo identity document.

(b) Identification and Verification of the Beneficial Owner

Where a customer is or acts on behalf of a legal person, legal arrangement, or trust, the Company must identify the beneficial owner — i.e. the natural person(s) who ultimately own or control the customer entity, including those exercising control through ownership of 25% or more, or through other means. The Company must take reasonable measures to verify the identity of the beneficial owner and understand the ownership and control structure of the customer.

(c) Purpose and Intended Nature of the Business Relationship

The Company must understand and, where appropriate, document the purpose for which the customer is using the platform and the nature of the activity expected. This information forms the baseline against which ongoing monitoring is assessed and enables detection of deviations from expected behaviour.

(d) Ongoing Monitoring

The Company must conduct ongoing due diligence on each business relationship, including scrutiny of transactions undertaken throughout the course of the relationship, to ensure that transactions are consistent with what the Company knows about the customer, their risk profile, and expected activity (including, where relevant, the source of funds). Risk profiles must be updated as new information becomes available.

8.3 Timing of CDD Measures

CDD measures must be applied before or during the establishment of a business relationship, or before the execution of an occasional transaction. Where it is not possible to complete CDD before

the business relationship commences, CDD may be completed during the establishment of the relationship, provided that:

- The ML/FT/FP risk is low.
- This is necessary to not interrupt the normal course of business.
- The measures are completed as soon as reasonably practicable after contact is first established.

Where CDD cannot be completed and the customer's account is subject to restrictions, the MLRO must decide whether to raise a Suspicious Transaction Report. Should CDD not be completed within the established timeframe, the customer's account will be frozen and further activity prevented. The MLRO must record the decision.

If the Company reasonably believes that performing CDD would tip off the customer that an UTR is being filed, the CDD process may be suspended and the report filed directly with the FIU via goAML.

8.4 Enhanced Due Diligence (EDD)

Enhanced Due Diligence must be applied whenever a higher risk of ML/FT/FP is identified. EDD triggers include, but are not limited to:

- Any customer categorised as a Foreign PEP (always EDD, regardless of other factors).
- Any customer categorised as a Domestic PEP or RCA where the risk assessment indicates elevated risk.
- Customers from or transacting with high-risk jurisdictions.
- Customers with complex or unusual transaction patterns that have no clear economic rationale.
- Non-face-to-face business relationships where technological controls are insufficient to mitigate identity fraud risk.
- Customers with unusual or disproportionate account activity relative to apparent income or source of funds.
- Any other customer whose risk profile the MLRO or senior management deems to require enhanced scrutiny.

EDD measures include, but are not limited to:

- Obtaining additional identification documents and verifying them from independent sources.
- Obtaining documentation to verify the customer's source of funds and/or source of wealth.
- Requiring senior management approval before establishing or continuing the business relationship.
- Conducting more frequent and intensive ongoing monitoring.
- Requiring enhanced transaction justification for unusual or large transactions.

8.5 Simplified Due Diligence (SDD)

Simplified Due Diligence may be applied where a customer, product, or transaction is assessed as presenting a low risk of ML/FT/FP, consistent with the risk-based approach and the Company's approved risk appetite. SDD may not be applied where there is any suspicion of ML/FT/FP, nor where the customer is a PEP or is connected to a high-risk jurisdiction.

Even where SDD is applied, the Company must still: (a) identify and verify the customer; (b) conduct ongoing monitoring; and (c) immediately escalate to standard or enhanced CDD if the risk level changes or any unusual activity is identified.

8.6 CDD for Existing Customers

The Company applies CDD measures to existing customers on a risk-sensitive basis. Periodic reviews are conducted as follows:

- High-risk customers: at least annually.
- Medium-risk customers: at least every two years.
- Low-risk customers: at least every three years.

Ad-hoc reviews are triggered by any material change in the customer's activity, risk profile, or circumstances, including: a significant change in transaction volumes or patterns; new adverse media or intelligence; change in PEP or sanctions status; or specific regulatory guidance.

8.7 Consequences of Failure to Complete CDD

Should a customer fail to complete the required CDD within the established timeframe, the Company will:

- Restrict the customer's account from any further activity.
- Freeze any funds held on the account.
- The MLRO will consider whether a Suspicious Transaction Report (STR/UTR) should be raised.
- Unless an STR has been filed and an appropriate holding period has elapsed, the account may be closed and deposited funds returned to the originating payment method, less any legitimate charges.
- All decisions and the basis for them must be recorded by the MLRO.

9. Reliance on Third Parties to Perform Customer Due Diligence

The Company does not rely on third parties to perform CDD measures on its behalf, in line with Curaçao regulatory requirements. The Company retains full responsibility for all CDD obligations and outcomes.

Where the Company uses third-party payment providers, the payment provider's verification of the account holder's name may be relied upon solely for the purpose of confirming the name on withdrawal payouts. The Company remains responsible for all other CDD obligations and must not treat the payment provider's checks as a substitute for the Company's own CDD requirements.

Any third-party service providers engaged in connection with AML/CFT/CFP obligations (such as screening software providers) must be subject to appropriate due diligence (see Section 19) and contractual obligations to comply with the Company's AML/CFT/CFP standards.

10. Payment Methods

The Company will not accept cash deposits or make cash payments in relation to customer activities.

The Company will only make use of payment methods offered by licensed financial institutions regulated by a European Economic Area (EEA) financial regulator, and will not accept funds originating from high-risk jurisdictions. Anonymous payment methods (including unregulated pre-paid cards and unregulated virtual assets) are treated as a high-risk factor requiring additional scrutiny.

Customer funds received are held in a player account, maintained separately and distinctly from the Company's own accounts.

The Company tracks all transactions carried out using accepted payment methods and identifies funds received from or remitted to customers, including transfers into or out of the player's account. The Company maintains sufficient controls to identify when due diligence thresholds have been reached.

Where possible, funds returned to customers are returned to the originating payment method. Where this is not possible due to the nature of the payment method or because the originating account is no longer available, payments are transferred only to a verified bank account in the customer's own name, following completion of the customer's due diligence process.

Transaction monitoring is conducted using internal systems and tools, supplemented by manual review processes.

11. High-Risk Jurisdictions

The Company conducts a geographical risk assessment on all countries from which it accepts customers. The assessment is completed using, at minimum, the following sources:

- FATF Jurisdictions under Increased Monitoring.
- FATF / CFATF High-Risk Jurisdictions subject to a Call for Action.
- CFATF Public Statement jurisdictions.
- EU list identifying high-risk third countries with strategic deficiencies.
- US Department of State Money Laundering Assessment (INCSR).
- Basel AML Index.
- Transparency International Corruption Perceptions Index.
- Countries sanctioned by the US OFAC.
- Countries identified by credible sources as providing funding or support for terrorist activities or as having terrorist organisations operating within them.

The Company maintains a documented list of countries classified as high risk and of those classified as low risk. This list is reviewed at least annually and updated promptly when the above sources are updated.

The Company does not accept customers resident in or whose funds originate from countries identified as high-risk on the above lists. This is enforced by blocking access from those countries. Where a customer's nationality, country of birth, or transactions are identified as connected to a FATF or CFATF-listed high-risk country, Enhanced Due Diligence is initiated.

12. AML/CFT/CFP Compliance Programme

12.1 Overview

The Company maintains a comprehensive AML/CFT/CFP Compliance Programme designed to prevent, detect, and report ML/FT/FP activity. The Programme comprises: (a) a system of internal policies, procedures and controls; (b) the appointment of an independent MLRO; (c) an employee screening and training programme; and (d) an independent audit function. The Programme is approved by the Board of Directors and reviewed at least annually.

12.2 Internal Controls

Internal control procedures are designed to comply with CGA Regulations and other applicable legislation. Internal controls include both automated controls within the gaming system software and manual controls operated by the Company's operations teams.

Automated / System Controls:

- Prevention of multiple accounts: System checks confirm whether the email address provided is unique, preventing a player from holding multiple accounts. The Company reserves the right to block or close any duplicate accounts at its discretion.
- Underage registration prevention: The system automatically prevents registrations that do not satisfy age verification requirements. No person under the legal gambling age may create an account.
- No cash and no credit policy: The system accepts credit card deposits only where a valid card with sufficient funds is presented. Players may participate in games only if they hold sufficient funds in their account. The Company does not accept cash and does not extend credit for gaming participation.
- Withdrawal name-matching: Payouts are only made to an account, card, wallet, or instrument held in the same name as the registered player. The Company relies on third-party payment providers to verify account holder names for bank transfer payouts.
- Anonymous account prohibition: Anonymous accounts and accounts in fictitious names cannot be created or maintained in the system.

Manual / Operational Controls (conducted by the operations team):

- Ongoing monitoring and assessment of players' risk indicators and changes in activity patterns.
- Daily review of deposits reports by the payment and risk department, with follow-up on suspicious transactions.
- Monitoring of large deposits and withdrawals, and patterns such as deposits followed immediately by withdrawals with insufficient gameplay.
- All withdrawal requests are checked and approved by the team before processing.
- Verification that the name on the withdrawal request matches the registered account holder and the destination bank account.
- Regular analysis of customer log activity for indicators of suspicious activity.
- Additional verification for suspicious deposits, transactions, or accounts, including outbound verification calls conducted in the player's language.
- Checking whether a player's details appear on local phone books, tax records, electoral registers, or other public databases.
- Requesting additional ID, proof of address, and bank statements where warranted.

Management maintains statistical data on the volumes generated by these procedures and performs monthly quality checks on agent work, sampling at least 25 cases per agent.

DC

12.3 Employee Screening

Prospective employees who will be involved in or connected to activities within the scope of this Policy must be screened before employment. The Company ensures that such individuals are fit and proper to occupy roles involving provision of services to customers. Third-party screening providers may be engaged.

The Company monitors the activities of employees during their employment to identify concerns of internal fraud or other criminal activity. The Company will respect the privacy of employees in doing so.

Employees are encouraged to report internal suspicious or fraudulent activity by colleagues directly to the MLRO and/or Directors. Anonymous reporting is available via an anonymous letter or email service.

12.4 Employee Training

Within an appropriate period of the commencement of employment, and at least annually thereafter, employees must receive AML/CFT/CFP training. Training shall include:

- General awareness of Money Laundering, Terrorism Financing, and Financing of Proliferation for all employees.
- The three stages of money laundering (Placement, Layering, Integration) and methods used to exploit the gaming sector.
- Specific guidance on the Company's measures, controls, policies, and procedures for employees in roles related to AML/CFT/CFP controls and compliance.
- An assessment to verify that the employee has understood the key points of the training. Employees who do not pass the assessment must undergo remedial training before resuming AML-relevant responsibilities.

Evidence of training provided to each employee (including the date, content covered, and assessment result) must be recorded and retained for at least five years. The MLRO is also required to attend annual refresher training and to keep up to date with developments in AML/CFT/CFP.

12.5 Independent Audit Function

The AML/CFT/CFP Compliance Programme must be subjected to independent testing and review at least annually. This review must be carried out by a party that is independent of the compliance/MLRO function — either a dedicated internal audit department or an appropriately qualified external auditor.

The independent auditor shall assess:

- The adequacy and effectiveness of the AML/CFT/CFP policies and procedures.
- The quality of CDD and ongoing monitoring processes.
- The effectiveness of transaction monitoring and STR/UTR escalation procedures.
- Staff training completeness and quality.
- Whether the BRA reflects the current risk environment.
- Compliance with the CGA Regulations and applicable legislation.

Findings, recommendations, and the Company's responses must be documented and presented to the Board of Directors. The MLRO must prepare and implement an action plan to address any deficiencies identified.

12.6 Examination by the Gaming Control Board

The Company shall cooperate fully with examinations and audits conducted by the Curaçao Gaming Authority (CGA) or any other competent authority. All records, policies, procedures, risk assessments, and transaction data must be made available upon request. The MLRO is the primary point of contact for regulatory examinations.

13. Suspicious Transaction Reporting and Unusual Transaction Reports

13.1 Reporting Obligations

The Company is required to adhere to the stipulations of the NORUT and to detect and report intended or unusual transactions. The following transactions or intended transactions are deemed unusual and must be reported to the FIU:

- Transactions which, in connection with money laundering, terrorism financing, or financing of proliferation, are reported to the Police or the Department of Justice.
- Transactions by or on behalf of a natural or legal person, group, or entity named on a sanctions list adopted pursuant to the Sanctions National Ordinance (N.G. 2014, no. 55).
- Transactions in the amount of NAf 4,000 or more, regardless of whether made in cash, by cheque or other payment instrument, electronically or by other non-physical means. This includes:
  - A cashless transaction (giro) of NAf 4,000 or more.
  - Accepting or releasing a deposit of NAf 4,000 or more at the client's request.
  - Sale to a customer of chips/tokens/credits in the amount of NAf 4,000 or more.
  - A cash-out in the amount of NAf 4,000 or more.
- Any transaction where, based on knowledge of the client and their activity, the Company has reasonable grounds to presume a connection to ML/FT/FP (subjective indicator).

13.2 Reporting Timeframes

- Objective indicator reports: All unusual transaction reports must be sent to the FIU without delay and within 48 hours after the transaction has been executed or an intention to transact has been identified.
- Subjective indicator reports: The period between execution (or intention) of a transaction and receipt of the report by the Compliance Officer must not exceed 24 hours. From receipt, the Compliance Officer has a maximum of 10 working days to conduct the relevant ML/FT/FP research. If, after the research period, a suspicion of ML/FT/FP remains, the Compliance Officer must report to the FIU within 48 hours.

13.3 goAML Reporting Platform

All Unusual Transaction Reports (UTRs) must be submitted to FIU Curaçao via the goAML platform, in accordance with the National Decree on rules for reporting unusual transactions (Landsbesluit goAML meldportaal). The MLRO is responsible for ensuring the Company is registered on goAML and that reports are filed in the required format.

13.4 Internal STR Process

An internal Suspicious Transaction Report (STR) must be sent directly to the MLRO whenever an employee has a suspicion that a customer is engaged in ML/FT/FP. The MLRO will assess the internal report and determine whether an external UTR to the FIU is required.

No employee may disclose to co-workers, line managers, or the customer that an STR or UTR has been or may be raised. Disclosing the fact of a report — or taking any action that could alert the subject — constitutes "tipping-off" and is a criminal offence. Employees who raise an STR must escalate directly to the MLRO and must not discuss the matter with any other person.

If the Company has a suspicion that performing CDD would tip off the customer, it may, after consulting the MLRO, choose not to pursue that CDD and should file a UTR with the FIU instead.

DC

14. Notifications of Fraud and Law Enforcement or Regulatory Authorities' Requests

The Company will record and take appropriate action whenever notification of fraud or requests by law enforcement or relevant regulatory authorities are received. The Company will follow due process to ensure such notifications or requests are processed without delay and will, within its abilities, assist such authorities effectively.

Notifications from law enforcement and regulatory authorities may also indicate areas where the Company's Responsible Gambling, Fraud, ML/FT/FP risk mitigation strategies require strengthening. Where gaps are identified, the Company will take immediate action to resolve them.

All reports must be sent without delay to the FIU via the goAML platform. The MLRO is responsible for managing all law enforcement and regulatory authority communications.

15. Employee Training

Employee training requirements are set out in full in Section 12.4 of this Policy. This section is incorporated by reference. All employees must complete AML/CFT/CFP training within an appropriate period after commencing employment and at least annually thereafter. Training records must be maintained and retained for at least five years.

16. Employee Screening

Employee screening requirements are set out in full in Section 12.3 of this Policy. This section is incorporated by reference.

17. Retention of Records

Customer and transactional data collected during the business relationship must be maintained for a minimum period of five (5) years from the end or termination of the customer relationship. The end of the customer relationship is defined as the later of: (a) the last day the customer effected any movement of funds to or from their account; or (b) the last successful login.

Records to be retained include, but are not limited to: identification and verification documents; CDD and EDD records; transaction history; STR/UTR records; training records; and BRA documentation.

Where statutory obligations under other laws, regulations, or specific regulatory requests require records to be kept for a longer period, the Company will comply accordingly. Documents will not be retained beyond the required obligations and will be securely deleted thereafter. All records must be made available to the CGA, FIU, or other competent authorities upon request.

18. Policy Distribution

All employees receive a copy of the AML/CFT/CFP Policy and all associated policies upon induction. Each year, once a review is completed and signed, the updated AML/CFT/CFP documents are circulated to all staff — including sub-contractors and third-party suppliers where applicable — by email, including a summary of material changes. Employees are required to acknowledge receipt and confirm their understanding of updated policies.

DL

19. Due Diligence for Third Parties

The Company has processes in place, where applicable, to carry out due diligence upon establishing a business relationship with third parties, in line with regulatory requirements and to ensure that the Company only works with reputable entities. Third-party suppliers and service providers involved in AML/CFT/CFP-related activities (including identity verification providers, payment processors, and screening software providers) must be subject to appropriate due diligence and contractual obligations requiring compliance with the Company's AML/CFT/CFP standards.

20. Policy URL

This Policy cannot be accessed online through the Company website. It is for internal use and is distributed directly to employees and relevant third parties as described in Section 18.

DC

21. Compliance and Consequences of Non-Compliance

The Company is obligated to comply with all regulations covered under Section 2 of this Policy. Should Deep Dive B.V. violate these regulations, the Company may be subject to disciplinary actions, legal implications, and significant business risks.

In situations of non-compliance, the following actions may be taken by the CGA or other competent authorities:

- Regulatory fines and financial penalties.
- Regulatory enforcement and sanctions.
- Suspension of operations.
- Revocation of the gaming licence.
- Criminal prosecution of responsible individuals.

Non-compliance by individual employees may result in disciplinary action up to and including dismissal, and potential personal liability under Curaçao criminal law.

Contact Information

Any questions regarding this Policy should be directed to:

- Name: Valentina Pirnau — MLRO
- Email: valentina.pirnau@herogaming.com
- Contact: +356 79009559

Appendix 1 — References

- CGA Regulations for Combating ML/FT/CFP — January 2025 (effective 9 January 2025, enforcement from 10 April 2025).
- United Nations — Financial Sanctions Consolidated List.
- European Union — Consolidated List of Sanctions.
- USA — OFAC Specially Designated Nationals (SDN) List.
- FATF — High-Risk Jurisdictions subject to a Call for Action (updated periodically).
- FATF — Jurisdictions under Increased Monitoring (updated periodically).
- CFATF — Public Statements.
- US Department of State — International Narcotics Control Strategy Report (INCSR).
- Basel Institute on Governance — Basel AML Index.
- Transparency International — Corruption Perceptions Index.
- Curaçao National Risk Assessment (NRA) — most recent published version.
- Curaçao Gaming Authority (CGA) website — for updates to Sanctions Decrees and Regulations.
- FIU Curaçao — goAML reporting portal.

Appendix 2 — Glossary of Terms

Term	Definition
AML	Anti-Money Laundering
BRA	Business Risk Assessment
Beneficial Owner	The natural person(s) who ultimately own or control a customer entity, including persons owning 25% or more of a legal person.
CAP	Customer Acceptance Policy
CDD	Customer Due Diligence — measures taken to identify and verify the customer, understand the purpose of the business relationship, and conduct ongoing monitoring.
CGA	Curaçao Gaming Authority (formerly the Gaming Control Board / GCB)
CFATF	Caribbean Financial Action Task Force
CFP / FP	Countering the Financing of Proliferation of Weapons of Mass Destruction / Financing of Proliferation
CFT	Countering the Financing of Terrorism
CRA	Customer Risk Assessment
DE	Designated Employee
EDD	Enhanced Due Diligence — additional CDD measures applied to higher-risk customers or situations.
FATF	Financial Action Task Force (www.fatf-gafi.org)
FIU	Financial Intelligence Unit — the national authority to which unusual transaction reports are filed.
FT	Financing of Terrorism
goAML	The FIU Curaçao's online platform for filing Unusual Transaction Reports.
INCSR	International Narcotics Control Strategy Report (US Department of State)
LOK	National Ordinance on Games of Chance (Landsverordening op de kansspelen)
ML	Money Laundering
MLRO	Money Laundering Reporting Officer
NOIS / LID	National Ordinance on Identification when Rendering Services (N.G. 2017, no. 92)
NORUT / LMOT	National Ordinance on the Reporting of Unusual Transactions (N.G. 2017, no. 99)

Term	Definition
NRA	National Risk Assessment — the Curaçao government's assessment of ML/FT/CFP risks.
OFAC	Office of Foreign Assets Control (US Department of the Treasury)
PEP	Politically Exposed Person
RBA	Risk-Based Approach
RCA	Relative or Close Associate (of a PEP)
SAR	Suspicious Activity Report
SDD	Simplified Due Diligence — a reduced level of CDD applied to lower-risk customers.
STR	Suspicious Transaction Report (internal)
UTR	Unusual Transaction Report (external report filed with the FIU via goAML)

Approval and Signatures

This Policy has been reviewed and approved on behalf of Deep Dive B.V.:

Role	Name	Signature / Date
MLRO	Valentina Pirnau	Signed by: Valentina Pirnau FB81912DE8374A0... 5/21/2026