

KYC Policy - Revision No. 2

Company Name: ENVISION DIGITAL N.V.

Registered address: Chuchubiweg 17, Willemstad, Curaçao

Registered Number: 140286

Main Domain: coinplay.com

Approved by: Director, CAPITAL TRUST CORPORATION N.V.

Compliance Officer: Serhii Yurchenko

Effective Date: 17.06.2026

Next Review Date: 17.06.2027

Principal Applicable Regulation: National Ordinance on the Identification when Rendering Services (LID, P.B. 2017, no. 92), the National Ordinance on the Reporting of Unusual Transactions (LMOT, P.B. 2017, no. 99), and the Regulations for the Combating of Money Laundering, the Financing of Terrorism and Proliferation of Weapons of Mass Destruction as of January 2025 (binding as of 10 April 2025), under the supervision of the Curaçao Gaming Authority (CGA). This Policy is to be read together with the Company's AML/CTF Policy.



1. Policy Statement and Purpose

ENVISION DIGITAL N.V., registered under number 140286 with its registered office at Chuchubiweg 17, Willemstad, Curaçao (the "Company"), operates the coinplay.com platform and is committed to implementing a full Know Your Customer (KYC) framework. This Policy sets out the Company's customer identification, verification and ongoing due diligence procedures, designed to prevent money laundering (ML), terrorist financing (TF), proliferation financing (PF) and fraud, and to ensure compliance with the applicable laws of Curaçao and the standards of the Curaçao Gaming Authority (CGA).

Customers are advised of this Policy at registration and on the Company's supporting non-transactional website.

2. Legal and Regulatory Framework

This Policy is adopted in compliance with:

- The National Ordinance on the Identification when Rendering Services (LID, P.B. 2017, no. 92);
- The National Ordinance on the Reporting of Unusual Transactions (LMOT, P.B. 2017, no. 99);
- The Sanctions National Ordinance (P.B. 2014, no. 55) and the Kingdom Sanction Act (P.B. 2016, no. 54);
- The Regulations for the Combating of Money Laundering, the Financing of Terrorism and Proliferation of Weapons of Mass Destruction, effective as of January 2025 (binding as of 10 April 2025);
- Guidance and standards issued by the Curaçao Gaming Authority (CGA).

This Policy must be read together with the Company's AML/CTF Policy.

3. Scope and Relationship to the AML/CTF Policy

This Policy applies to all Customers of the Company and governs the practical identification, verification, due diligence and ongoing monitoring measures applied throughout the customer lifecycle, from registration to account closure. It operationalizes the Customer Risk Assessment (CRA), Customer Acceptance Policy (CAP), and CDD/EDD requirements set out in the Company's AML/CTF Policy. Where this Policy and the AML/CTF Policy are inconsistent, the AML/CTF Policy prevails.

The Company's business model does not permit player accounts to be opened or operated by legal entities; this Policy therefore applies exclusively to natural persons.

4. Definitions

- KYC: Know Your Customer — the process of identifying and verifying a Customer's identity.
- CDD: Customer Due Diligence.

- EDD: Enhanced Due Diligence.
- SoF / SoW: Source of Funds / Source of Wealth.
- PEP: Politically Exposed Person.
- MLRO / CO: Compliance Officer / Money Laundering Reporting Officer.
- FIU: Financial Intelligence Unit Curaçao.
- STR: Suspicious Transaction Report / unusual transaction report, filed with FIU Curaçao via the goAML portal.
- CGA: Curaçao Gaming Authority.
- Customer: a natural person of the approved age who registers to participate in games of chance offered by the Company.

Terms not defined in this Policy carry the meaning given to them in the Company's AML/CTF Policy.

5. Roles and Responsibilities

5.1 Management

Senior management approves this Policy, allocates resources for its implementation, and is informed periodically of KYC-related risks and escalations.

5.2 Compliance Officer (MLRO) / Compliance Department

The Compliance Officer (MLRO) has overall ownership of this Policy. The Compliance Officer approves High Risk onboarding decisions, EDD outcomes, account blocking/closure decisions taken on AML/CFT grounds, and determines whether a matter is reported to FIU Curaçao.

5.3 Operations / Customer Support

The Operations and Customer Support teams collect, review and verify Customer-submitted documents in accordance with Sections 7 and 8, and escalate doubtful or incomplete cases to the Compliance Department without delay.

5.4 Anti-Fraud Department

The Anti-Fraud Department investigates suspected document fraud, identity theft, and fraudulent account activity referred to it under Section 13, and reports its findings to the Compliance Officer.

5.5 External Service Providers

The Company may rely on external identity verification, sanctions/PEP screening, or transaction monitoring providers. Any such reliance is subject to Section 7 (Reliance on Third Parties) of the AML/CTF Policy; ultimate responsibility for all KYC decisions remains with the Company.

6. Risk-Based Approach and Customer Risk Classification

Each Customer is assigned a Low, Medium or High risk rating at registration and throughout the relationship, consistent with the Customer Risk Assessment (CRA) under the AML/CTF Policy,

based on factors including registration jurisdiction, PEP/sanctions/adverse media screening results, payment methods used, and transactional behaviour. The level of verification and due diligence applied under this Policy is proportionate to the Customer's risk rating, as set out in Sections 7 to 11.

7. Onboarding Process and Identity Verification Workflow

7.1 Registration and Initial Disclosure

At registration, and generally on the Company's supporting non-transactional website, Customers are informed that the Company uses online verification tools and that, where these tools cannot satisfy the applicable verification criteria, identity and address verification documents will be requested.

7.2 Identification Documents

The Company requires a valid official identification document bearing a photograph of the holder, being one of: a driving licence; an identity card; a travel document or passport; or any other document designated by the Ministry of Finance of Curaçao.

7.3 Address Verification Documents

Where requested by the Company, verification of the Customer's residential address may be carried out using one of: a valid official identity document; a recent utility bill; a recent account statement or reference letter issued by a credit or financial institution; correspondence from a central or local government authority, department or agency; or any other document issued by an independent agency.

7.4 Phone Number Verification

Verification of the Customer's identity also includes mandatory confirmation of the Customer's phone number.

7.5 Verification Criteria for Identity Documents

An identification document is considered valid for KYC purposes where: it shows the Customer's name, photograph, date of birth and citizenship; this information fully matches the data held in the Customer's profile; and the document is currently valid (not expired). The Company checks submitted documents for signs of alteration or editing and, where necessary, requests a selfie of the Customer holding the identification document to confirm that the document belongs to the person who registered the account.

The Company reserves the right to request additional documentation at any time where reasonably necessary to complete its AML/KYC checks and to meet applicable compliance standards.

8. Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD)

8.1 Standard CDD

The identification and verification measures described in Section 7 constitute the Company's baseline CDD, applied to all Customers in accordance with their risk rating.

8.2 Enhanced Due Diligence (EDD)

EDD is applied where a Customer is classified as High Risk, reaches the thresholds set out in Section 10, uses high-risk payment methods, is identified as a PEP, or where there is suspicion of fraud, money laundering or terrorist financing. EDD measures include: in-depth review of the Customer's profile and transaction history; verification of source of funds and/or source of wealth under Section 8.3; Compliance Officer approval prior to continuing the relationship; and more frequent re-verification under Section 11.

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

In some cases, the Company requires additional proof of funds to verify that a Customer is using their own funds to participate in gaming on the Company's platform. SoF documentation evidences the origin of funds used for a specific transaction; SoW documentation evidences the Customer's overall financial standing. Such documentation is requested in proportion to the size and nature of the transaction concerned, and is mandatory for High Risk Customers and Customers meeting the EDD thresholds in Section 10.

9. PEP, Sanctions and Adverse Media Screening

At registration, and on an ongoing basis throughout the relationship, the Company screens each Customer against:

- Sanctions lists, including the UN Security Council Consolidated List, EU Sanctions, UK OFSI Sanctions, OFAC Sanctions, and the Curaçao Sanctions National Ordinance list;
- PEP databases; and
- Adverse media sources.

A confirmed sanctions list match results in immediate rejection of the registration or blocking of the account, and is reported in accordance with the AML/CTF Policy. A PEP match or adverse media finding results in High Risk classification and the application of EDD under Section 8.2. Re-screening is performed periodically and upon any material change to the Customer's profile.

10. Thresholds for KYC Triggers

The identity and address verification documents described in Section 7 must be obtained before processing any transaction(s) reaching a cumulative threshold of XCG 4,000 in deposits and/or withdrawals, calculated on the basis set out in the AML/CTF Policy. Source of Funds / Source of Wealth documentation under Section 8.3 must be obtained where a single transaction, or a series of linked transactions, reaches or exceeds XCG 5,000.

The above documentation may also be requested earlier than these thresholds, irrespective of amount, where the Company suspects fraudulent activity, money laundering or terrorist financing.

11. Ongoing Monitoring and Re-Verification

The Company performs ongoing monitoring of Customer identity and account activity, including:

- periodic re-verification of identity documents according to risk rating: Low Risk every 36 months, Medium Risk every 24 months, High Risk every 12 months;
- re-verification upon a change of address, contact details, or payment method;
- re-verification upon expiry of a previously submitted document; and
- re-verification upon reclassification of the Customer to a higher risk rating.

The Compliance Department determines, on a risk-sensitive basis, whether a change in Customer information requires full re-verification or may be logged without further action.

12. Betting Activity and Winnings Verification

The Company reviews Customer betting activity to detect possible manipulation, collusion or other irregularities. Where there is uncertainty regarding the legitimacy of winnings credited to a Customer's account, the Company contacts the relevant game or odds provider to verify the bet(s) concerned before releasing the related funds.

13. Document Authenticity and Suspicion Handling

The Company checks all submitted documents for signs of alteration or forgery. Where there are reasonable grounds to suspect that a document is invalid, altered or fraudulent, the matter is escalated to the Anti-Fraud Department and the Compliance Officer (MLRO) without delay, in accordance with Section 14.

14. Escalation Procedures and Decision-Making Authority

Doubtful documents, suspected fraud, suspicious transactions, or any other trigger identified under this Policy follow the escalation path: Operations/Customer Support → Anti-Fraud Department (where fraud is suspected) → Compliance Department → Compliance Officer (MLRO).

The Compliance Officer (MLRO) has sole authority to:

- approve onboarding or continuation of the relationship with High Risk Customers;
- approve the outcome of an EDD review;
- decide on restriction, freezing, blocking or closure of an account under Section 15; and
- determine whether an STR (unusual transaction report) should be filed with FIU Curaçao.

15. Blocking, Restriction and Account Closure

Where evidence of suspicious transactions is found on a Customer's account — including cash deposits from questionable sources (for example, where the sender's details do not match the account holder), or any action showing signs of fraud, including refunds or cancelled payments — the Company applies the following measures, depending on severity:

- Restriction — deposits and/or withdrawals are paused, while the Customer may continue to use their existing account balance for gameplay;

- Freeze — the account, including gameplay, is fully suspended pending the outcome of an internal investigation; and
- Blocking or closure — the account is permanently blocked or closed and related payments are cancelled, following confirmation of fraud, ML/TF involvement, or another Non-Acceptable Customer attribute under the AML/CTF Policy.

The Company may request additional information where the withdrawal method differs from the deposit method, and may apply the restriction or freeze measures above if the Customer refuses to provide such information.

In the course of an investigation, the Company may request additional copies of identity documents, copies of the bank cards used to fund the account, payment documents, and other evidence confirming the lawful possession and legal origin of funds, including original documents where necessary.

The Company applies Enhanced Due Diligence to Customers classified as High Risk, including those registered from or transacting via high-risk jurisdictions, in accordance with Section 8.2 and the AML/CTF Policy.

The Company's refusal to perform, or withholding of, a transaction considered suspicious (including the blocking or closure of a Customer's account) does not give rise to civil liability of the Company for failure to fulfil its obligations to the Customer, provided the Company acts in good faith and in accordance with applicable law.

16. Recordkeeping

All identification documents, verification records, screening results, and decisions taken under this Policy are retained for at least five (5) years from the end of the business relationship, consistent with the Company's AML/CTF Policy, and are made available to the CGA and FIU Curaçao upon lawful request.

17. Processing Timeframes

The processing of a KYC check may require up to a maximum of seventy-two (72) hours. The Customer is required to provide requested documents within five (5) working days of the request.

Failure to provide the requested documents within this period triggers the restriction or freeze measures described in Section 15. Continued failure to provide the requested documentation within thirty (30) days from the date of the request results in termination of the business relationship, in accordance with the Company's AML/CTF Policy.

18. Approvals

Approved 17.06.2026

Director

CAPITAL TRUST CORPORATION N.V.

Compliance Officer



Serhii Yurchenko

19. Version History

Revision No. 1 — effective 02.04.2026

Revision No. 2 — effective 17.06.2026 (current)

