

OPTIM DEVELOPMENT B.V.

Anti-Money Laundering And Terrorism Financing Prevention Policy

Effective Date:

20.05.2025

Next Review Date:

10.01.2026



Anastasiia Latypova, MLRO

TABLE OF CONTENTS

1. POLICY STATEMENT	3
2. PURPOSE	3
3. AUDIENCE	4
4. DEFINITIONS	4
5. POLICY IMPLEMENTATION	6
5.1 Business Risk Assessment	6
5.2 Customer Risk Assessment	7
5.3 Customer Acceptance Policy	8
5.4 Customer Due Diligence	8
5.5 Ongoing Monitoring	9
5.6 Reliance on Third Parties	10
5.7 Reporting of Unusual Transactions	10
5.8 AML Compliance Program	10
6. COMPLIANCE AND CONSEQUENCES OF NON-COMPLIANCE	11
7. RELATED INFORMATION	12
8. CONTACT INFORMATION	12

1. POLICY STATEMENT

Optim Development B.V. is firmly committed to the highest standards of integrity and compliance in preventing the use of its products and services for money laundering, terrorist financing, or any form of financial crime. The Company fully adheres to the applicable legislation and regulatory guidance issued by the Curaçao Gaming Control Board (GCB), including the National Ordinance on Identification when Rendering Services (NOIS), the National Ordinance on the Reporting of Unusual Transactions (NORUT), the Sanctions National Ordinance, and applicable EU AML Directives and FATF Recommendations.

This Policy outlines the principles, responsibilities, and internal controls adopted by the Company to detect and prevent money laundering and terrorist financing. It establishes a risk-based framework for identifying, assessing, and mitigating ML/TF risks across the Company's operations and relationships with customers, agents, third-party providers, and business partners.

The Policy applies to:

- All services and operations of Optim Development B.V., including online platforms and digital infrastructure;
- All directors, officers, employees, agents, and contractors of the Company;
- Any third parties acting on behalf of the Company.

The Company prohibits any activities that facilitate money laundering or the funding of terrorist or criminal activity. Optim Development B.V. maintains a zero-tolerance approach to non-compliance with AML/CTF obligations and ensures that all applicable transactions and customers are subject to appropriate due diligence, monitoring, and regulatory reporting.

2. PURPOSE

The purpose of this Policy is to establish a comprehensive and operational framework to detect, prevent, and report activities related to money laundering, terrorist financing, and other forms of financial crime that may affect Optim Development B.V., its partners, clients, or the integrity of the financial system.

This Policy is designed to ensure compliance with:

- Curaçao legislation, including NOIS, NORUT, the Sanctions National Ordinance;
- The regulations and directives issued by the Curaçao Gaming Control Board (GCB);
- The Financial Action Task Force (FATF) 40 Recommendations;
- The European Union Directives on Anti-Money Laundering (AMLD4, AMLD5, AMLD6);
- Applicable international sanctions regimes (UN, EU, OFAC).

It supports the Company in:

- Applying a risk-based approach to ML/TF risk management;
- Implementing proportionate customer due diligence measures;
- Reporting suspicious activity in a timely and effective manner;
- Promoting a culture of compliance and accountability;
- Preserving the Company's integrity, license, and reputation.

The Policy also aims to protect the Company, its stakeholders, and the gaming ecosystem from being misused as a channel for criminal or terrorist activity, and to ensure that its business remains fully transparent, lawful, and trustworthy.

3. AUDIENCE

This Policy is intended for all internal and external stakeholders who perform functions relevant to the Company's compliance with anti-money laundering and counter-terrorist financing obligations. This includes personnel involved in customer interaction, transaction processing, compliance, risk management, and decision-making functions.

The Policy must be clearly understood and followed by all individuals whose roles impact the Company's exposure to financial crime risks, regardless of their location, employment status, or contractual engagement.

4. DEFINITIONS

The following terms are used throughout this Policy and should be interpreted as defined below:

Anti-Money Laundering (AML) – A set of procedures, laws, and regulations designed to stop the generation of income through illegal actions. It includes customer due diligence, reporting of suspicious transactions, and internal controls.

Business Risk Assessment (BRA) – The organization-wide analysis of ML/TF risks based on products, services, customers, geographies, and delivery channels.

Counter-Terrorist Financing (CTF) – Measures aimed at detecting, preventing, and disrupting the financing of terrorism and related activities.

Customer Acceptance Policy (CAP) – The formal criteria under which the Company accepts or rejects a customer, based on risk profile, verification status, and regulatory requirements.

Customer Due Diligence (CDD) – The process of identifying and verifying the identity of a customer, and assessing the risks associated with that customer.

Customer Risk Assessment (CRA) – The structured evaluation of an individual customer's ML/TF risk profile based on factors such as geography, behavior, payment methods, and source of funds.

Curaçao Gaming Control Board (GCB) – The supervisory authority for licensed gaming operators in Curaçao, responsible for enforcing compliance with AML/CTF requirements.

Enhanced Due Diligence (EDD) – A more in-depth KYC process applied to high-risk customers or transactions, including verifying the source of funds and wealth, and increased ongoing monitoring.

Financial Intelligence Unit (FIU) – The national agency responsible for receiving, analyzing, and reporting unusual or suspicious financial activity. In Curaçao, this is FIU-MOT.

Know Your Customer (KYC) – The broader process of gathering and verifying information about a customer to assess risk and comply with AML/CTF obligations.

Money Laundering (ML) – The process by which criminals disguise the original ownership and control of the proceeds of criminal conduct by making such proceeds appear to be derived from a legitimate source.

Money Laundering Reporting Officer (MLRO) – The designated person within the Company responsible for overseeing the AML/CTF framework, handling internal disclosures, and submitting reports to the FIU.

National Ordinance on Games of Chance (LOK) – The primary legal framework regulating the gaming sector in Curaçao, under which licensing and compliance are governed.

National Ordinance on Identification when Rendering Services (NOIS) – The Curaçao law requiring proper identification and verification of customers before services are provided.

National Ordinance on the Reporting of Unusual Transactions (NORUT) – The Curaçao law requiring the reporting of certain types of transactions to the FIU.

Office of Foreign Assets Control (OFAC) – The U.S. governmental body that administers and enforces economic and trade sanctions.

Politically Exposed Person (PEP) – An individual who holds or has held a prominent public function and therefore poses a higher risk due to potential involvement in bribery or corruption.

Sanctions Lists – Officially issued lists by authorities such as the UN, EU, or OFAC identifying individuals, entities, or countries subject to restrictive measures.

Suspicious Transaction Report (STR) – A report submitted to the FIU when there is a reason to suspect that funds are related to criminal activity or terrorism financing.

Terrorist Financing (TF) – The process of providing financial support to terrorist organizations or persons who encourage, plan, or carry out terrorist acts.

Two-Factor Authentication (2FA) – A security process that requires users to verify their identity using two different authentication methods.

Unusual Transaction Report (UTR) – A report submitted to the FIU when a transaction is considered unusual under the applicable regulatory criteria, even if no suspicion of a criminal offense arises.

5. POLICY IMPLEMENTATION

Optim Development B.V. implements this AML/CTF Policy through a structured and risk-based framework that integrates legal requirements, internal governance, operational procedures, and technology tools. The Compliance Department, under the oversight of the Money Laundering Reporting Officer (MLRO), is responsible for the execution and continuous development of this framework.

Key implementation functions include conducting risk assessments, applying due diligence measures, monitoring customer activity, reporting suspicious transactions, and ensuring internal staff awareness and accountability. The policy is applied consistently across all business units and jurisdictions in which the Company operates, and all departments involved in customer-facing or financial operations are required to cooperate with compliance-related directives issued under this Policy.

The MLRO reports directly to the Board of Directors and has the authority to implement changes, coordinate audits, and escalate risks identified through monitoring or regulatory feedback. All procedures implemented under this Policy are reviewed periodically and updated as needed to reflect evolving regulatory obligations and risk exposures.

5.1 Business Risk Assessment

Optim Development B.V. conducts a comprehensive Business Risk Assessment (BRA) at least annually, or more frequently if there are significant changes in the business model, product offering, technology, regulatory landscape, or external threat environment. The BRA forms the basis for the Company's risk-based approach and ensures that AML/CTF controls are appropriate and proportionate.

The BRA aims to identify and assess the inherent ML/TF risks associated with the Company's core activities, including but not limited to:

- **Product and service offerings:**

Includes risk assessments of individual game types (e.g., RNG casino, sports betting, live dealer), loyalty programs, bonuses, and payout mechanics. Certain products may present elevated risks due to faster turnover, high transaction volumes, or potential use for layering activities. New product features, including instant win formats or anonymous game modes, are subject to prior AML risk review.

- **Customer types and profiles:**

Different customer segments (e.g., recreational players vs. high-value VIPs) present different risk levels. The Company also considers occupation, declared source of funds, deposit behavior, and previous account history (e.g., multiple accounts, rapid deposit-withdrawal patterns). Players with crypto-linked payment activity or those using proxy/VPN are also flagged for heightened review.

- **Geographic exposure:**

The Company evaluates countries based on FATF grey/black lists, EU and UN sanctions, and internal

red flags. Players residing or transacting from high-risk jurisdictions, or countries with weak AML controls or conflict zones, trigger enhanced scrutiny. Country-of-payment origin and location of access (IP address) are factored separately.

- **Payment methods:**

Risks vary depending on whether payment flows are traceable (e.g., bank transfer) or anonymous (e.g., prepaid cards, crypto wallets). BRA includes analysis of volume caps, chargeback activity, mismatch of deposit and withdrawal methods, and use of intermediary wallets. New payment providers must undergo AML due diligence before integration.

- **Emerging risks:**

Includes evolving threats such as:

- use of virtual assets and decentralized exchanges;
- social engineering and account takeover patterns;
- cross-border fraud linked to politically unstable or sanctioned regions;
- changes in Curaçao or EU legislation that create new exposure points;
- adoption of AI or automated gameplay (botting) that may mask transaction trails.

The assessment takes into account the nature, scale, and complexity of the Company's activities, as well as known typologies and guidance issued by the Curaçao Gaming Control Board, FATF, and other international bodies.

Results of the BRA are documented and reviewed by the Compliance Department and the MLRO. They are presented to the Board of Directors for approval and are used to:

- Calibrate Customer Risk Assessment methodologies;
- Adjust internal controls and thresholds for monitoring;
- Inform the scope and frequency of compliance reviews and audits;
- Support regulatory reporting and license obligations.

5.2 Customer Risk Assessment

Optim Development B.V. applies a structured Customer Risk Assessment (CRA) methodology at the onboarding stage and throughout the business relationship. Each customer is assigned a risk score based on weighted criteria grouped into key risk categories. The outcome determines the level of due diligence (standard or enhanced) and frequency of monitoring.

Risk Categories and Evaluation Criteria:

Geographic Risk:

Denied: customers from jurisdictions prohibited under Curaçao license conditions, including:

Australia, Austria, Belgium, France, Germany, Italy, Netherlands, Spain, United Kingdom, United States, and Dutch overseas territories (Aruba, Bonaire, Curaçao, Saba, Sint Eustatius, Sint Maarten);

Rejected: customers from FATF high-risk or blacklisted jurisdictions;

Enhanced due diligence (EDD) required: customers from countries under OFAC/EU/UN sanctions or jurisdictions with weak AML enforcement;

Medium/low risk: EU/EEA countries and jurisdictions with established AML/CFT frameworks.

Product and Transaction Risk:

Higher risk: customers involved in high-turnover games (e.g., live casino, slots with rapid cycles);

Higher risk: significant net-loss behavior over short periods;

Lower risk: customers with low betting frequency and limited deposit amounts.

Payment Method Risk:

Denied: use of anonymous or non-traceable methods (e.g., prepaid cards without KYC, masked wallets);

Enhanced checks: use of crypto wallets, intermediated e-wallets (e.g., Skrill, Neteller) without account match;

Medium/low risk: SEPA, SWIFT, cards under customer's name.

Customer Profile Risk:

Higher risk: declared source of funds in cash-intensive businesses (real estate, crypto, gambling, adult content, etc.);

Higher risk: PEPs, public figures, or persons linked to negative media;

Lower risk: salaried employees with verifiable income and ID.

Behavioral and Interface Risk:

Flags: repeated deposit/withdrawal without gameplay; multiple accounts from same IP/device; VPN usage;

Flags: inconsistent KYC data (e.g., age mismatch, unverifiable documents);

Lower risk: verified customers with consistent play and activity pattern.

Scoring and Risk Rating:

- Each sub-factor is scored on a scale (1 = low risk, 20 = high risk; 50 = extra high-risk trigger);
- Final score determines risk rating: Low / Medium / High;
- High-risk customers are subject to EDD and management approval.

5.3 Customer Acceptance Policy

Optim Development B.V. applies a documented and risk-sensitive Customer Acceptance Policy (CAP), ensuring that only customers with acceptable risk profiles are permitted to open and maintain accounts.

Customers shall not be accepted if:

- They are residents of jurisdictions prohibited by Curaçao license terms or international sanctions (see Section 5.2);
- They are listed on sanctions databases (UN, EU, OFAC, etc.) or internal blacklists;
- They are unwilling or unable to provide complete and accurate KYC documentation;
- Their source of funds or source of wealth cannot be verified upon request;
- They attempt to use anonymous, non-traceable or fraudulent payment methods;
- They are under the age of 18 or the applicable legal age in their jurisdiction.

Customers may be accepted only with EDD and management approval if:

- They are identified as Politically Exposed Persons (PEPs);
- They reside or transact from jurisdictions flagged as high-risk (but not prohibited);
- They exhibit unusual patterns during onboarding (e.g., mismatched identity data, proxy use);
- They declare high-risk occupations or involvement in sensitive industries (e.g., crypto, gambling, adult content, real estate).

Other provisions:

- Where a customer fails verification or exhibits suspicious behavior during onboarding, the account shall not be activated and may be closed with funds withheld until risk resolution;
- The Company retains the right to terminate any business relationship if the customer's risk level changes or becomes unacceptable after onboarding;
- All acceptance decisions, especially for high-risk or flagged cases, must be documented and subject to MLRO review.

5.4 Customer Due Diligence

Optim Development B.V. applies a risk-based Customer Due Diligence (CDD) process to verify the identity and legitimacy of each customer prior to allowing access to its services. The CDD process ensures compliance with NOIS, FATF Recommendations, and relevant international AML standards.

CDD measures include:

- **Verification of identity:**
 - Full name, date of birth, nationality, and unique ID number;
 - Valid government-issued photo ID (passport, national ID, or driver's license)
 - Real-time document verification and selfie check (where applicable).
- **Verification of address:**
 - Proof of residence (e.g., utility bill, bank statement, government correspondence) dated within 3–6 months;
 - Address must match registration data and IP geolocation (flag if mismatched).

- **Verification of contact details:**
 - Email and phone number validation;
 - Two-factor authentication (2FA) enabled for login or withdrawals.
- **Assessment of financial profile:**
 - Initial review of declared occupation and estimated income;
 - Source of funds for deposits exceeding EUR 1,000 or equivalent;
 - Source of wealth if total deposits exceed EUR 10,000 or customer presents high risk.

Enhanced Due Diligence (EDD) is triggered when:

- Customer is identified as a PEP, sanctioned individual, or linked to adverse media;
- Customer is from a high-risk or sanctioned jurisdiction (see Section 5.2);
- Customer uses crypto, third-party wallets, or shows unusual payment behavior;
- Customer's identity cannot be reliably verified or documents are inconsistent;
- Customer deposits large amounts without gaming activity (possible layering).

Timing and verification rules:

- All standard CDD must be completed prior to the first withdrawal and no later than 30 days from registration (whichever comes first);
- Accounts with incomplete verification are suspended after 30 days and may be closed;
- EDD customers must be approved by Compliance and MLRO before any withdrawals.

Ongoing obligations:

- CDD must be updated every 12–24 months based on customer risk rating;
- CDD documents must be refreshed if expired, altered, or flagged as invalid;
- All CDD and EDD documentation is retained for a minimum of 5 years after account closure.

5.5 Ongoing Monitoring

Optim Development B.V. maintains a continuous and risk-sensitive monitoring program to detect suspicious or unusual customer behavior throughout the business relationship.

Monitoring activities include:

- **Transaction monitoring:**
 - Real-time analysis of deposits, withdrawals, and betting patterns;
 - Alerts based on thresholds (e.g., EUR 1,000+, rapid turnover, repeated withdrawals);
 - Ratio analysis (e.g., deposit-to-bet, deposit-to-withdrawal mismatches).
- **Behavioral monitoring:**
 - Account access from high-risk IPs or geographies (e.g., via VPN, TOR, proxies);
 - Changes in device fingerprint or geolocation without justification;

- Frequent password resets or failed login attempts (possible account compromise).
- **Documentation and profile updates:**
- Regular review of customer profiles based on risk rating (e.g., every 12–24 months);
- Immediate review if red flags are triggered (e.g., deposit spikes, inactivity → large withdrawal);
- Mandatory refresh of expired or unverifiable CDD documents

Sanctions and PEP list re-screening:

- Periodic re-screening against updated UN/EU/OFAC/PEP lists;
- Immediate action if positive match identified (account flagged and escalated to MLRO).

Outcomes and actions:

- All alerts are reviewed by the Compliance Department or escalated to MLRO as needed;
- Accounts may be temporarily suspended during investigation of alerts;
- Monitoring results are used to re-evaluate customer risk scores and trigger EDD if necessary;
- Confirmed suspicious activity leads to STR submission to FIU Curaçao.

5.6 Reliance on Third Parties

Optim Development B.V. may rely on regulated third-party entities for the performance of specific CDD components, such as identity verification and document collection. Such reliance is only permitted where:

- The third party is subject to equivalent AML/CFT regulations (e.g., EU-licensed institutions, FATF-compliant providers);
- A written agreement is in place, granting the Company access to all collected CDD data on request;
- The Company retains full responsibility for AML compliance and must be able to demonstrate the adequacy of the third party's procedures to the regulator.

Reliance on unregulated, informal, or non-compliant parties is strictly prohibited.

5.7 Reporting of Unusual Transactions

Optim Development B.V. ensures that all Unusual or Suspicious Transactions are reported to the FIU Curaçao (MOT) in accordance with the NORUT.

- Employees must escalate red flags to the MLRO immediately;
- The MLRO reviews and, where applicable, submits a report to the FIU within 15 business days;
- Urgent cases are reported without delay and before execution if required;
- Customers must not be informed about any report or internal investigation (tipping-off is strictly prohibited).

5.8 AML Compliance Program

Optim Development B.V. maintains a formal, risk-based AML/CTF Compliance Program designed to prevent the use of its services for money laundering and terrorist financing.

The Program includes:

- This AML/CTF Policy and internal procedures approved by the Board of Directors;
- Appointment of an independent and qualified MLRO with sufficient authority and resources;
- Ongoing risk assessments (BRA, CRA) and updates to controls based on findings;
- Transaction monitoring, customer screening, and STR/UTR reporting protocols;
- Annual staff training on AML obligations and red flag awareness;
- Periodic internal reviews and independent audits to test program effectiveness.

The AML Compliance Program is reviewed at least once a year or upon material changes in law, business model, or risk exposure. Responsibility for oversight and execution rests with the MLRO, under the supervision of the Board.

Compliance with this Policy is mandatory for all staff, management, and relevant third parties acting on behalf of Optim Development B.V.

Any breach of this Policy may result in:

- Internal disciplinary action, including dismissal;
- Suspension or termination of contracts with external partners;
- Reporting to regulatory or law enforcement authorities;
- Civil or criminal penalties under applicable law.

The Company enforces a zero-tolerance approach to deliberate or negligent violations of AML/CTF obligations. All breaches must be promptly reported to the MLRO and recorded in accordance with internal escalation procedures

6. COMPLIANCE AND CONSEQUENCES OF NON-COMPLIANCE

Compliance with this Policy is mandatory for all staff, management, and relevant third parties acting on behalf of Optim Development B.V.

Any breach of this Policy may result in:

- Internal disciplinary action, including dismissal;
- Suspension or termination of contracts with external partners;
- Reporting to regulatory or law enforcement authorities;
- Civil or criminal penalties under applicable law.

The Company enforces a zero-tolerance approach to deliberate or negligent violations of AML/CTF obligations. All breaches must be promptly reported to the MLRO and recorded in accordance with internal escalation procedures.

7. RELATED INFORMATION

This Policy is based on and aligned with the following legal and regulatory documents:

- National Ordinance on the Reporting of Unusual Transactions (NORUT);
- National Ordinance on Identification when Rendering Services (NOIS);
- Sanctions National Ordinance;
- National Ordinance on Games of Chance (LOK);
- Curaçao Gaming Control Board AML/CFT Regulations (January 2025);
- FATF Recommendations;
- EU AML Directives (AMLD IV, V, VI).

It also refers to internal policies such as the Company's Code of Conduct, Privacy Policy, and AML Training Plan.

8. CONTACT INFORMATION

For any questions or concerns regarding this Policy or AML/CTF compliance in general, please contact:

Email: compliance@optim-development.org

Registered office: Fransche Bloemweg 4, Curaçao