

Anti-Money Laundering and Counter-Terrorist Financing (AML/CTF) Policy

Twins Games N.V.

License Number: 165516

Effective Date: February 2025

Next Review Date: February 2026

Registered Office: Zuikertuintjeweg Z/N, Zuikertuin Tower, Willemstad, Curaçao

Website: <https://www.apuesterapido.com/>

Contact: contact@apuesterapido.com

Designated AML Compliance Officer (AMLCO): [Name – to be confirmed]

1. Policy Statement

Twins Games N.V. (“the Company”) is firmly committed to maintaining the highest standards of integrity, transparency, and compliance in the fight against money laundering (ML), terrorist financing (TF), and any activity that may threaten the integrity of the gaming industry.

This policy outlines the Company’s framework for compliance with the Curaçao Gaming Authority (CGA) Anti-Money Laundering and Counter-Terrorist Financing regulations, as well as the Directive (EU) 2018/843 of the European Parliament, on the prevention of money laundering and limitation of the use of cash.

Twins Games N.V. strictly prohibits and actively prevents the use of its services for laundering proceeds of crime or for the financing of terrorism. Every employee, agent, and contractor of the Company is expected to adhere to the obligations set out in this document and to promptly report any activity that may appear suspicious or inconsistent with normal gaming behavior.

The Company's management fully supports this policy and ensures the allocation of adequate resources to enforce and maintain compliance at all operational levels.

2. Purpose

The purpose of this policy is to:

- Establish a clear and practical framework for the prevention, detection, and reporting of ML and TF activities;
- Define the roles and responsibilities of all personnel in maintaining AML/CTF compliance;
- Ensure that Twins Games N.V. complies with all applicable laws, directives, and guidelines issued by the CGA and other relevant authorities;
- Protect the reputation, stability, and integrity of the Company, its customers, and the gaming industry;
- Ensure that appropriate systems and internal controls are in place for customer due diligence (CDD), risk assessment, record-keeping, and suspicious activity reporting.

The Company acknowledges that effective AML/CTF compliance is an ongoing process requiring continual assessment, improvement, and training. This policy is therefore reviewed annually or upon any material regulatory or operational change.

3. Audience

This policy applies to:

- All employees of Twins Games N.V. and its affiliated entities;
- Directors, senior management, and Board Members;
- Contractors and external service providers (e.g., payment processors, marketing agencies, KYC verification vendors);
- Any third party that provides operational, financial, or compliance-related services on behalf of the Company.

Every employee or third party engaged with Twins Games N.V. must read, understand, and comply with this policy.

Failure to comply may result in disciplinary, contractual, or legal consequences.

4. Definitions

For the purpose of this policy, the following definitions apply:

- Money Laundering (ML):

The act of concealing the origin of funds obtained from illegal activity, by transferring or converting them into seemingly legitimate assets or transactions. It includes:

- The conversion, transfer, or concealment of assets derived from criminal activity;
- The acquisition, possession, or use of assets known to originate from criminal activity;
- Participation, conspiracy, facilitation, or attempts to commit such acts.

- Terrorist Financing (TF):

The act of providing or collecting funds, directly or indirectly, with the intention or knowledge that they will be used to carry out terrorist acts.

- Customer Due Diligence (CDD):

The process of verifying a customer's identity and assessing the level of risk they pose based on their activity, origin of funds, and other indicators.

- Enhanced Due Diligence (EDD):

Additional checks applied to high-risk customers or transactions, including those involving Politically Exposed Persons (PEPs), sanctioned countries, or complex structures.

- Politically Exposed Person (PEP):

An individual who holds or has held a prominent public position (e.g., government official, head of state, senior executive of a state-owned company), as well as their family members and close associates.

- Suspicious Transaction Report (STR):

A report submitted to the Financial Intelligence Unit (FIU) of Curaçao whenever there is knowledge or suspicion that funds are related to ML or TF.

- AML Compliance Officer (AMLCO):

The designated officer responsible for the daily oversight of AML/CTF controls, reporting obligations, and staff training within Twins Games N.V.

5. Policy Implementation

5.1 Business Risk Assessment (BRA)

Twins Games N.V. performs an Enterprise-Wide Risk Assessment (EWRA) at least once per year to evaluate exposure to ML/TF risks across all business areas.

This assessment considers:

- Products and services offered (sports betting, casino, payment methods, bonuses);
- Geographical regions of operation and customer base;
- Customer behavior patterns and transaction volumes;
- Use of third-party providers or affiliates;
- Technological systems and vulnerabilities.

The AMLCO ensures that the findings of the EWRA are documented, approved by management, and that mitigation measures—such as limits, verification triggers, and AI monitoring—are implemented accordingly.

Adjustments to the AML framework are made whenever new products, countries, or payment methods are introduced.

5.2 Customer Risk Assessment (CRA)

Each customer is assigned a risk level—low, medium, or high—based on multiple criteria, including nationality, payment type, frequency of transactions, and prior behavior.

Risk Group Examples:

- Region 1 (Low Risk): Standard markets with stable regulations.
- Region 2 (Medium Risk): Countries where enhanced verification applies (Stage 2 from USD 1,000 and Stage 3 from USD 2,500).

- Region 3 (High Risk): Countries banned by the Company due to sanctions or AML exposure.

Automated systems evaluate transactional patterns to detect anomalies such as rapid withdrawals, deposits with no gaming activity, or mismatched currencies. These are flagged for manual review by the AMLCO's team.

5.3 Customer Acceptance Policy (CAP)

To establish a secure and transparent customer base, Twins Games N.V. enforces a three-stage verification framework:

1. Stage 1 — Basic Verification

Mandatory for all users prior to any withdrawal.

Requires full name, date of birth, nationality, gender, and full residential address.

Conducted automatically through the site's registration form and validated electronically.

2. Stage 2 — Intermediate Verification (USD 2,000+)

Triggered when cumulative deposits or withdrawals exceed USD 2,000.

Requires:

- A photo of a valid government-issued ID alongside a handwritten note with six random digits;
- Electronic verification of identity and address through two independent databases;
- If electronic checks fail, a proof of address (utility bill, bank statement, or government document issued within 3 months).

3. Stage 3 — Enhanced Verification (USD 5,000+)

Triggered when cumulative deposits or withdrawals exceed USD 5,000.

Requires submission of a Source of Funds (SOW) document, such as:

- Proof of salary, inheritance, investments, or business income;
- Bank or credit card statement confirming ownership;
- Declaration explaining the legitimate origin of funds.

If a customer refuses or fails to provide the requested documentation, their account is suspended, and a review is initiated by the AMLCO. At any point, and for any reason, Twins Games N.V. may enforce additional due diligence.

5.4 Customer Due Diligence (CDD)

All customers undergo identity verification before being permitted to withdraw funds.

The process may include :

- Document validation: ID, passport, or driver's license;
- Facial recognition: Photo of the customer holding the ID and random digits;
- Payment method verification: Deposits and withdrawals must use the same method to prevent third-party usage;
- PEP & Sanction Screening: Automated screening against global PEP databases and international sanctions lists (EU, UN, OFAC).

If the verification process fails, then the user account is frozen, the AMLCO is notified, and an internal assessment determines whether to file an STR with the FIU Curaçao.

5.5 Ongoing Monitoring

Monitoring is continuous and risk-based.

Twins Games N.V. employs AI-powered behavioral analysis supervised by human compliance officers to identify:

- Deposits followed by immediate withdrawals;
- Frequent changes of nationality, payment method, or currency;
- Multiple accounts linked by shared details or IP addresses;
- Unusual login locations or device patterns.

Each alert is manually reviewed and documented.

Where necessary, accounts are temporarily blocked pending clarification or escalation to the FIU.

5.6 Reliance on Third Parties

The Company collaborates only with licensed and regulated payment providers and data verification partners that comply with AML/CTF standards equivalent to those of Curaçao and the EU.

Third parties are subject to written agreements ensuring:

- KYC and transaction screening are performed effectively;
- Audit rights for Twins Games N.V.;
- Immediate reporting of suspicious activities.

Ultimate responsibility for AML compliance always remains with Twins Games N.V. and cannot be outsourced.

5.7 Reporting of Unusual Transactions

All employees and contractors must remain vigilant for signs of suspicious or unusual transactions.

Indicators include:

- Attempts to use multiple payment accounts or third-party cards;
- Inconsistencies between deposits, income, and gameplay;
- Refusal to complete verification or provide source of funds;
- Activity inconsistent with customer profile or historical behavior.

Once detected, the employee must immediately notify the AMLCO, who will review the case and decide whether to:

1. File an Internal Suspicious Activity Report (SAR), and/or
2. Submit a Suspicious Transaction Report (STR) to the FIU Curaçao.

No employee should inform the customer of such reporting (“tipping off” is strictly prohibited).

5.8 AML Compliance Program

The Company’s AML Program includes:

- A documented system of policies, procedures, and controls;
- Annual and ad-hoc training for employees, tailored to their responsibilities;
- Regular internal audits and reporting to senior management;
- Record retention for at least 10 years from the end of the business relationship;
- Encryption and secure storage of all data in compliance with the EU Data Protection Directive (95/46/EC).

The AMLCO has full authority to enforce this program and ensure adherence to Curaçao AML/CTF regulations.

6. Compliance and Consequences of Non-Compliance

Failure to comply with this policy, whether intentional or due to negligence, may result in:

- Disciplinary action, including suspension or dismissal;
- Termination of contracts with third-party providers or partners;
- Regulatory fines or license suspension imposed by the CGA;
- Criminal liability where applicable under Curaçao or EU law.

The Company’s reputation, operational integrity, and regulatory standing depend on strict compliance with this policy.

All employees are therefore expected to act with diligence and report any potential breach immediately.

7. Related Information

This policy must be read in conjunction with other legal, regulatory, and internal documents that form part of the Company's compliance ecosystem. The following resources and legal references are applicable:

Regulatory and Legal Framework

- Curaçao AML/CTF Guidelines (CGA) – The principal regulatory standard governing licensed gaming operators in Curaçao;
- EU Directive (EU) 2015/849 – On the prevention of the use of the financial system for the purposes of money laundering or terrorist financing;
- Regulation (EU) 2015/847 – On information accompanying transfers of funds;
- Law of 18 September 2017 – On the prevention of money laundering and the limitation of the use of cash;
- United Nations Sanctions Lists and EU Sanctions Regulations – Including measures restricting dealings with designated individuals or entities;
- Data Protection Directive 95/46/EC – On the protection of individuals with regard to the processing of personal data.

Internal Policies and Procedures

- Know Your Customer (KYC) and Verification Procedures – Detailing the three-stage verification system;
- Responsible Gaming Policy – Ensuring player protection and ethical gaming practices;
- Information Security Policy – Governing data storage, encryption, and access control;
- Employee Code of Conduct – Establishing standards for ethical behavior, confidentiality, and reporting obligations;
- Internal Audit Framework – Defining periodic compliance reviews and corrective measures.

These related documents are accessible internally through the Company's compliance portal and are reviewed annually to ensure full alignment with AML/CTF legislation.

8. Contact Information

For any questions, concerns, or reports regarding this AML/CTF Policy, employees, partners, and regulators may contact:

Designated AML Compliance Officer (AMLCO)

Twins Games N.V.

Zuikertuintjeweg Z/N, Zuikertuin Tower

Willemstad, Curaçao

 Email: contact@apuesterapido.com

 Website: <https://www.apuesterapido.com/>

The AMLCO has unrestricted authority to request information, suspend accounts, or escalate cases to the Financial Intelligence Unit (FIU) of Curaçao as required by law.

All communications with the AMLCO are treated with the strictest confidentiality and handled in accordance with the Company's data protection standards.

9. Policy History

Review Schedule

This policy shall be reviewed:

- Annually, or
- Immediately upon any material change in AML/CTF legislation, risk exposure, or operational model of Twins Games N.V.

All revisions are approved by both the Board of Directors and the AML Compliance Officer before publication.

10. Policy URL and Public Access

The official and most up-to-date version of this policy is available online at:

<https://www.apuesterapido.com/informacoes/politica-aml>

Customers and regulators may consult this page to verify the Company's AML commitments, obtain contact details, or review the latest effective version.

Archived versions of this document are maintained internally for audit and transparency purposes.