

Anti Money Laundering & Know Your Customer Policy

AML Policy of Prism Sentinel N.V.

Last updated: April 22nd, 2025

Anti-Money Laundering (AML) and Know Your Customer (KYC) Policy for Cash Deposits and Withdrawals

Introduction

www.mintdice.com is operated by Prism Sentinel N.V., registered at Chuchubiweg 17, Curaçao, with Company Registration number 146440 (0). As a Curaçao-based entity, Prism Sentinel N.V. is committed to complying with the anti-money laundering (AML) and counter-terrorist financing (CFT) regulations of Curaçao.

Objective of the AML Policy

The objective of this AML policy is to ensure the highest level of security for all users and customers of www.mintdice.com by verifying their identity and preventing the platform from being used for money laundering or terrorist financing. This includes a multi-step verification process to confirm that customer details are accurate and that deposit and withdrawal methods are legitimate. The policy accounts for varying risk levels based on customer nationality, payment methods, and transaction types, in line with Curaçao's risk-based AML/CFT framework.

Prism Sentinel N.V. implements reasonable measures to control and mitigate money laundering risks, dedicating appropriate resources to compliance. The AML program is designed to comply with:

- **National Ordinance on Combatting Money Laundering and the Financing of Terrorism (AB 2019, no. 25)**
- **National Ordinance on Identification when Rendering Services (LID)**
- **National Ordinance on the Reporting of Unusual Transactions (NORUT)**
- **Provisions and Guidelines on the Detection and Deterrence of Money Laundering and Terrorist Financing** issued by the Centrale Bank van Curaçao en Sint Maarten (CBCS)
- Recommendations of the **Financial Action Task Force (FATF)** and the **Caribbean Financial Action Task Force (CFATF)**

Definition of Money Laundering

Money laundering is defined under Curaçao law as:

- The conversion or transfer of property, knowing it is derived from criminal activity, to conceal or disguise its illicit origin or to assist any person involved in such activity to evade legal

- consequences.
- The concealment or disguise of the true nature, source, location, disposition, movement, or ownership of property, knowing it is derived from criminal activity.
- The acquisition, possession, or use of property, knowing at the time of receipt that it was derived from criminal activity.
- Participation in, association with, attempts to commit, or aiding, abetting, facilitating, or counseling the commission of the above actions.

Money laundering is considered an offense even if the predicate criminal activity occurred outside Curaçao, consistent with FATF standards.

Organization of the AML Program

In accordance with Curaçao's AML/CFT legislation, Prism Sentinel N.V. has designated its senior management as the highest authority responsible for AML compliance. An **AML Compliance Officer (AMLCO)** is appointed to oversee the implementation and enforcement of AML policies and procedures, reporting directly to senior management.

AML Policy Changes and Implementation

Any significant changes to the AML policy require approval from Prism Sentinel N.V.'s senior management and the AMLCO. Policies are reviewed annually or as needed to align with updates to Curaçao's AML/CFT regulations and FATF recommendations.

Customer Identification and Verification (KYC)

Customer identification is a cornerstone of Curaçao's AML/CFT regime. The following multi-step verification process is implemented:

Step One Verification

- **Requirement:** Mandatory for all customers before any withdrawal.
- **Process:** Customers must complete a form providing:
 - First name and surname
 - Date of birth
 - Nationality
 - Gender
 - Full residential address
- **Verification:** Data is cross-checked electronically using at least one reputable database to ensure accuracy. If electronic verification fails, customers must provide a government-issued document (e.g., certificate of registration) to confirm their residence.

Step Two Verification

- **Requirement:** Mandatory for customers depositing or withdrawing over USD 1,000 or transferring over USD 500 to another user.
- **Process:** Customers must submit:
 - A clear image of a government-issued ID (e.g., passport, driver's license, or national ID)

- card) alongside a handwritten note displaying a six-digit randomly generated number.
- The ID must show the customer's name, date of birth, nationality, and gender, with other details optionally obscured for privacy.
- Verification:** The submitted ID is electronically verified against Step One data. If verification fails, customers must provide proof of address (e.g., a utility bill or bank statement issued within the last three months).

Step Three Verification

- Requirement:** Mandatory for customers depositing or withdrawing over USD 3,000 or transferring over USD 1,500 to another user.
- Process:** Customers must provide evidence of their **Source of Wealth (SOW)**, which may include:
 - Proof of business ownership
 - Employment records (e.g., payslips or employment contract)
 - Inheritance documentation
 - Investment records
 - Family wealth documentation
- Verification:** The AMLCO reviews SOW documents to ensure the legitimacy of funds. Additional documents may be requested if the origin of wealth is unclear. Transactions are held until verification is complete.

Proof of Address

- Requirement:** Required if electronic verification fails or for Step Two/Three verification.
- Process:** Customers must submit a recent document (issued within the last three months) such as:
 - Utility bill (electricity, water, etc.)
 - Bank statement
 - Government-issued document confirming residence
- Verification:** Documents must clearly show the customer's name, address, and issuance date, with all four corners visible.

Banking Details

To further verify identity and financial status, customers must use the same payment method for deposits and withdrawals up to the deposited amount. A bank wire or credit card statement may be 植物 to confirm the payment method's legitimacy.

Risk Management

Prism Sentinel N.V. adopts a risk-based approach, categorizing customers into three risk levels based on their country of residence:

- Low Risk:** Customers from jurisdictions with robust AML/CFT regimes (e.g., FATF-compliant countries). Standard verification applies.
- Medium Risk:** Customers from jurisdictions with moderate AML/CFT deficiencies.

Verification thresholds are lowered:

- Step Two: Deposits/withdrawals over USD 500 or transfers over USD 250.
- Step Three: Deposits/withdrawals over USD 1,500 or transfers over USD 750.
- Customers converting cryptocurrencies are treated as medium risk.
- **High Risk:** Customers from jurisdictions listed by the FATF as high-risk or non-cooperative are banned. The high-risk list is updated regularly based on CBCS and FATF guidance.

Additional Measures

- An AI-driven system, overseen by the AMLCO, monitors transactions for unusual patterns (e.g., rapid deposits and withdrawals, inconsistent banking details, or nationality changes).
- Human employees conduct manual reviews of AI-flagged transactions and perform random checks on high-risk accounts.
- Customers must use consistent payment methods for deposits and withdrawals to prevent layering.

Enterprise-Wide Risk Assessment (EWRA)

Prism Sentinel N.V. conducts an annual EWRA to identify and mitigate AML/CFT risks specific to its operations, including:

- Services offered (e.g., online gaming and cryptocurrency transactions)
- Customer profiles and geographic locations
- Transaction types and delivery channels
- Emerging risks (e.g., virtual assets)

The EWRA informs the AML policy and is updated to reflect regulatory changes and industry best practices.

Ongoing Transaction Monitoring

Transaction monitoring is conducted on three levels to detect unusual or suspicious activity:

1. **First Line of Control:** Trusted Payment Service Providers (PSPs) with robust AML policies perform initial KYC checks before deposits reach www.mintdice.com.
2. **Second Line of Control:** An automated system monitors transactions in real-time, flagging those that deviate from the customer's profile (e.g., large or rapid transactions). Employees review flagged transactions, considering:
 - Customer KYC data
 - Financial behavior
 - Transaction counterparties
3. **Third Line of Control:** Manual reviews are conducted for high-risk or suspicious accounts, with additional due diligence as needed.

Reporting of Unusual Transactions

Under Curaçao's NORUT, www.mintdice.com is required to report unusual transactions to the Financial Intelligence Unit (FIU) of Curaçao via the goAML portal. Internal procedures outline:

- When staff must report unusual transactions to the AML team.
- How the AML team analyzes transactions using a risk-based methodology.
- Criteria for escalating reports to the FIU within 10 working days, as required by law.

The AML team may:

- File a report with the FIU if a transaction is deemed suspicious.
- Terminate business relationships with customers involved in suspicious activity.

Record Keeping

In compliance with Curaçao regulations:

- Customer identification records are retained for at least **7 years** after the business relationship ends.
- Transaction records are retained for at least **7 years** from the date of the transaction.
- Data is stored securely, both offline and online, with encryption to protect customer privacy.

Training

All employees involved in financial transactions or customer interactions receive mandatory AML/CFT training, including:

- Annual training on Curaçao's AML/CFT laws and FATF standards.
- Onboarding sessions for new employees, covering www.mintdice.com's AML policies.

Training is delivered by an AML specialist from Prism Sentinel N.V.'s AML team and tailored to employees' roles.

Auditing

Internal audits are conducted regularly to assess AML/CFT compliance, with reports submitted to senior management and the AMLCO. Audit findings inform policy updates and corrective actions.

Data Security

Customer data is protected in accordance with Curaçao's data protection laws and international best practices:

- Data is encrypted and stored securely.
- Data is not shared with third parties unless required by law or to prevent money laundering.
- Data may be shared with the FIU or other authorities if mandated by Curaçao law.

Contact Us

For questions about our AML and KYC Policy, please contact:

- **Email:** support@mintdice.com

For complaints regarding AML/KYC checks or account-related issues, please contact:

- **Email:** support@mintdice.com

If you have any complaints about our AML and KYC Policy or about the checks done on your Account and your Person, please contact us:

By email: security@mintdice.com