

Anti-Money Laundering & Counter-Terrorist Financing Policy

AML / CFT POLICY

Anti-Money Laundering & Counter-Terrorist Financing Policy

(Effective for elitbahis.com)

elitbahis.com is operated by **Venus International B.V.**, a company incorporated under the laws of Curaçao with Company Number **164106** and licensed by the Curaçao Gaming Authority ("CGA") under license number **OGL/2024/1127/0766**, in accordance with the National Ordinance on Games of Chance (Landsverordening op de kansspelen, P.B. 2024, no. 157).

This AML/CFT Policy outlines the measures we take to prevent our platform from being used for **Money Laundering (ML)**, **Terrorist Financing (TF)** or **Financing of Proliferation (FP)**, in line with the Curaçao NOIS, NORUT, Sanctions National Ordinance, Kingdom Sanctions Act, and the **CGA's January 2025 AML/CFT Regulations**.

1. Policy Statement

elitbahis.com is fully committed to preventing and detecting all forms of ML/TF/FP.

We apply a **risk-based AML program** that includes:

- Business Risk Assessment (BRA)
- Customer Risk Assessment (CRA)
- Customer Due Diligence (CDD)
- Enhanced Due Diligence (EDD) where required
- Ongoing monitoring
- Sanctions & PEP screening
- Reporting Unusual Transactions to FIU Curaçao
- Record-keeping
- Employee AML training

2. Purpose

This policy ensures compliance with Curaçao's AML laws and CGA AML Regulations, including:

- The National Ordinance on Identification when Rendering Services (NOIS)
- The National Ordinance on Reporting Unusual Transactions (NORUT)
- Sanctions National Ordinance / Kingdom Sanction Act
- CGA AML/CFT Regulations (January 2025) – full framework for casinos

3. Scope & Audience

This policy applies to:

- All employees of Venus International B.V.
 - Compliance Officers
 - KYC/Payments staff
 - Contractors and service providers handling player data or payments
-

4. Key Definitions

Aligned with Annex 1 of the CGA Regulations: Money Laundering, Terrorist Financing, Customer Due Diligence, Beneficial Owner, PEP, Source of Funds, Source of Wealth, Unusual Transactions, etc.

5. AML Policy Framework

5.1 Business Risk Assessment (BRA)

We maintain a documented BRA identifying risks related to:

- Customer profiles
- Geographical exposure
- Products and payment methods
- Delivery channels (online, remote onboarding)
- Technology risks (new systems/products)

As required by CGA II.2.1

Reviewed annually or upon major business/market changes.

5.2 Customer Risk Assessment (CRA)

CRA is performed **before or during onboarding**, assigning *low / medium / high* ML/TF risk levels.

Risk indicators include:

- Multiple income sources
- High spending patterns
- PEP status

- High-risk countries (FATF lists)
- Anonymous or high-risk payment methods
- Irregular transactional behavior

(CGA Risk Factors II.2.2 & II.2.3)

5.3 Customer Acceptance Policy (CAP)

We do not accept:

- Anonymous players
- Sanctioned individuals/entities
- Players who refuse required CDD/EDD
- Third-party funded accounts without clear UBO verification

CAP integrates all PEP and sanctions screening obligations.

5.4 Customer Due Diligence (CDD)

Minimum CDD is conducted **at account creation**, including:

- Full name, residential address, date of birth (minimum low-risk data)
- Identity verification using government-issued documents
- PEP & sanctions screening (UN, EU, local lists)
- Verification of source of funds when needed

(CGA III.2.1 Identification & Verification)

CDD must be completed **when cumulative financial transactions reach NAf. 4,000**.

Until CDD is complete: deposits/withdrawals are blocked.

5.5 Enhanced Due Diligence (EDD)

EDD is triggered for:

- PEPs
- High-risk countries
- High-value transactions
- Irregular or complex transaction patterns
- Players using high-risk products or anonymous methods

EDD measures include:

- Proof of income / source of wealth
- Additional ID verification
- Senior management approval
- Increased ongoing monitoring

(CGA III.4)

5.6 Ongoing Monitoring

Our system continuously monitors:

- Deposit/withdrawal patterns
- Changes in behavior inconsistent with risk profiles
- Large or complex transactions
- Use of third-party wallets/cards
- Re-verification on document expiry

(CGA III.2.4 On-Going Monitoring)

5.7 Sanctions & PEP Screening

All players are screened against:

- **UN Consolidated List**
- **EU Sanctions Lists**
- **Curaçao local sanctions lists**
- **PEP databases**
- **FATF High-Risk Jurisdictions**

(CGA III.2.1 & III.6)

Screening is done at onboarding and periodically.

5.8 Reliance on Third Parties

If relying on a third-party KYC provider:

- They must be regulated and AML-compliant
- Data must be accessible immediately upon request
- The casino retains full responsibility for customer risk assessment and monitoring

(CGA III.9)

5.9 Reporting Unusual Transactions (FIU Curaçao)

We detect, document and report all unusual transactions as required by NORUT and CGA Section IV:

- NAf. 5,000+ transactions (cashless/cash-out/deposits/chips/credits)
- Suspicious patterns
- Transactions linked to sanctioned persons
- Any activity with presumed ML/TF indicators

All reports are submitted via **FIU Curaçao's goAML Portal**.

Tipping-off the player is strictly prohibited.

5.10 Record Keeping

We retain:

- CDD/KYC data
- Transaction records
- BRA, CRA, CAP
- FIU reports
- Internal investigation notes

for **minimum 5 years** as mandated by NORUT and CGA Section IV.3.

5.11 AML Training

Staff receive AML/CFT training including:

- ML/TF methods in gambling
- CDD/EDD procedures
- Recognizing unusual transactions
- Sanctions & PEP identification
- FIU reporting process

(CGA Section V.4)

Annual refreshers are mandatory.

5.12 Independent Audit

An independent audit of the AML program is performed annually, per CGA V.5 requirements.

Findings are reported to senior management with corrective action deadlines.

5.13 Termination of Business Relationship

The platform will:

- Block or terminate accounts when CDD cannot be completed
- Return funds to the original deposit method
- File FIU reports when suspicion of ML/TF exists

(CGA III.8)

6. Non-Compliance Consequences

Violations of this policy may result in:

- Account suspension/closure
- Mandatory reporting to FIU
- Regulatory penalties
- Criminal investigation (per Curaçao law)

(Required by AML Template Section 6)

7. Contact

For AML/CFT matters:

Compliance Department – Venus International B.V.

Email: compliance@elitbahis.com

8. Policy Review

Reviewed annually or upon regulatory changes.

Latest Update: **November 2025**