

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

Winholding B.V.

Effective Date: June 30, 2025 | Review Date: June 30, 2026

1. Policy Statement

Winholding B.V. is committed to ensuring full compliance with all applicable anti-money laundering (AML) and counter-terrorism financing (CTF) laws and regulations in Curaçao. This policy establishes procedures for identifying, mitigating, and reporting money laundering and terrorist financing risks associated with its operations and client base. It applies to all business units, employees, and affiliates of Winholding B.V.

2. Purpose

This policy outlines Winholding B.V.'s approach to preventing and detecting money laundering and terrorism financing in accordance with Curaçao regulations, including those enforced by the CGA and the FIU Curaçao. It provides employees with guidance on identifying suspicious activities and fulfilling legal obligations.

3. Audience

This policy applies to all employees, management, subcontractors, and third-party partners engaged with Winholding B.V. and involved in handling customer onboarding, financial transactions, compliance, or data management.

4. Definitions

Key terms include Money Laundering, Terrorist Financing, Customer Due Diligence (CDD), Enhanced Due Diligence (EDD), Suspicious Transaction Report (STR), Politically Exposed Person (PEP), and Ultimate Beneficial Owner (UBO).

5. Policy Implementation

5.1 Business Risk Assessment

An annual Business Risk Assessment (BRA) is conducted to identify ML/TF risks across products, services, delivery channels, and customer segments. The BRA informs the AML program and helps prioritize control measures in line with CGA requirements.

5.2 Customer Risk Assessment

Customer Risk Assessments (CRA) are performed at onboarding and periodically reviewed. Each customer is rated as low, medium, or high risk based on profile, geography, and transaction behavior.

5.3 Customer Acceptance Policy

Winholding B.V. only engages customers who meet risk thresholds defined by the CRA and CAP. The CAP prohibits relationships with sanctioned individuals, anonymous users, and high-risk entities without full EDD.

5.4 Customer Due Diligence

CDD is performed at onboarding and upon transaction thresholds of NAF 4,000 or suspicion. Identification, address verification, UBO checks, and PEP/sanctions screening are required. Funds may be frozen and reported if anomalies are identified.

5.5 Ongoing Monitoring

Customer transactions are monitored using automated systems and manual review. Alerts are generated for abnormal patterns, with periodic re-verification of CDD for high-risk clients.

5.6 Reliance on Third Parties

When CDD is outsourced, Winholding B.V. ensures third parties are subject to equivalent AML laws, with access rights to documentation and retained compliance responsibility.

5.7 Reporting of Unusual Transactions

Employees escalate suspicious activity to the MLRO. STRs are filed to FIU Curaçao where applicable. Internal reports and decisions are logged and retained for at least five years.

5.8 AML Compliance Program

The AML Program is reviewed annually and designed to address specific risks identified in the BRA. It defines training standards, audit scope, reporting protocols, and procedures for account blocking.

6. Compliance and Consequences of Non-Compliance

Violations may lead to disciplinary action, contract termination, legal prosecution, and reputational damage. Compliance is mandatory and monitored continuously.

7. Related Information

CGA AML Policy (Jan 2025), FIU Curaçao Reporting Guidelines, PEP Screening Procedures, STR Template, CRA Checklist.

8. Contact Information

Compliance Officer | Email: Nathan@winholdings.co.uk | Tel: +599 9 8432772

9. Policy History

This is the first version of the AML/CTF Policy for Winholding B.V., effective June 30, 2025.

10. Policy URL

Only available offline

11. B2C Operator Considerations

11.1 Nature of Operations

Winholding B.V. is a B2C (Business-to-Consumer) operator, providing gaming and betting services directly to individual customers. As such, the company is exposed to a broad range of customer profiles and financial behaviors, necessitating strong customer verification and transaction monitoring protocols.

11.2 B2C-Specific AML Risks

The following ML/TF risks are particularly relevant in a B2C context:

- Use of stolen or synthetic identities.
- Fraudulent credit/debit card transactions.
- Structuring (smurfing) of deposits to avoid detection.
- Use of multiple accounts or proxy players.
- Self-laundering through minimal-play withdrawals.
- Use of third-party or prepaid payment methods.

11.3 Customer Due Diligence Measures

Winholding B.V. performs identity verification for all players upon registration and/or when financial thresholds are reached. Enhanced verification (EDD) is conducted for high-risk jurisdictions, high-value players, and PEPs. Tools may include biometric checks, video liveness tests, and AI-driven fraud detection models.

11.4 Transaction and Gameplay Monitoring

As part of its B2C model, Winholding B.V. performs transaction monitoring systems that flag:

- Rapid deposit and withdrawal cycles with little gameplay.
- Use of multiple payment methods or accounts.
- Unusual gameplay behavior suggestive of money movement rather than entertainment.
- Players consistently operating just below verification thresholds.

11.5 Age and Identity Controls

Strict age verification controls are in place to ensure no minor access. Digital identity tools are employed to validate name, age, and geographic location. Accounts flagged for inconsistencies are suspended until reviewed by the Compliance team.

11.6 Player Education and Transparency

Winholding B.V. maintains transparency with players regarding AML requirements. Where EDD or document requests are initiated, the rationale is clearly explained to the customer. A privacy policy ensures compliance with GDPR and local data protection laws.