



Anti-Money Laundering Policy

AML/CFT compliance framework in accordance with CGA requirements, FATF recommendations, and Curaçao national legislation.

v1.0

☐ Draft

☰ TABLE OF CONTENTS

1.0 Purpose & Scope

This Anti-Money Laundering (AML) and Counter-Terrorism Financing (CFT) Policy establishes the framework, procedures, and controls designed to prevent the use of the operator's platform for money laundering, terrorism financing, or any other financial crime.

This policy applies to all employees, contractors, agents, and third-party service providers acting on behalf of the operator. It covers all products and services offered by FHP Network B.V., which exclusively provides online poker and poker variations. No sports betting, no statically established casino games where the odds are against the players, such as blackjack, roulette, baccarat, slots, etc), live dealer products, or any other form of gambling other than poker is offered. All payment processing activities related to poker operations are also covered by this policy.

The operator is committed to full compliance with applicable AML/CFT legislation, CGA regulatory requirements, and international standards including FATF Recommendations.

2.0 Legal & Regulatory Framework

This policy is designed to comply with the following legislation and regulations:

- Curaçao National Ordinance on the Reporting of Unusual Transactions (NORUT)
- Curaçao National Ordinance on Identification when Rendering Financial Services (NOIRS)
- CGA Anti-Money Laundering Regulations and Guidance
- Financial Action Task Force (FATF) Recommendations
- EU Anti-Money Laundering Directives (where applicable)
- United Nations, EU, and OFAC sanctions regimes

3.0 Risk Assessment

The operator conducts a comprehensive, documented risk assessment covering:

- **Customer Risk:** Player profile, source of funds, geographic location, PEP status, transaction patterns
- **Product/Service Risk:** Game types, betting patterns, bonus abuse potential, peer-to-peer features
- **Geographic Risk:** Jurisdictions with higher ML/TF risk (FATF grey/black lists), sanctioned countries
- **Channel Risk:** Online-only operations, mobile platform, third-party deposits
- **Payment Method Risk:** Cryptocurrency, e-wallets, prepaid cards, bank transfers

The risk assessment is reviewed at least annually, or more frequently following significant changes to products, markets, or regulations. The risk assessment informs the level of CDD and monitoring applied.

4.0 Customer Due Diligence (CDD)

FHP Network B.V. requires all players to complete full KYC verification before any deposit. This mandatory pre-deposit verification process includes:

- **Age Verification:** Confirmation that the player is at least 18 years of age, verified through the identity and facial recognition process
- **Identity Verification:** Government-issued photo ID (passport, national ID card, driving license)
- **Proof of Address:** Utility bill, bank statement, or official correspondence dated within 3 months
- **Facial Recognition:** Advanced facial recognition software is used to verify the customer's authenticity by matching the submitted ID against a live biometric check, ensuring the account holder is genuine and present

Source of Funds (SOF): SOF inquiries are conducted on a case-by-case basis at the sole discretion of FHP Network B.V. Each player is approached individually for SOF based on FHP Network B.V.'s own internal risk assessment. There is no single fixed threshold — the decision to request SOF documentation is made following an individualized review of each player's account activity, deposit patterns, and risk profile.

5.0 Enhanced Due Diligence (EDD)

Enhanced Due Diligence is applied in the following circumstances:

- Customer identified as a Politically Exposed Person (PEP) or PEP associate
- Customer from a high-risk jurisdiction (FATF grey/black list)
- Unusual or suspicious transaction patterns identified
- High-value players (VIP) exceeding defined deposit thresholds

- Complex or unusual transaction structures
- Adverse media screening alerts

EDD measures include: enhanced source of funds/wealth verification, senior management approval for continued relationship, increased monitoring frequency, and periodic relationship reviews.

6.0 Transaction Monitoring

The operator employs automated transaction monitoring systems to detect suspicious activity. Monitoring includes:

- Real-time monitoring of deposits, withdrawals, and wagering activity
- Pattern analysis for structuring, layering, and unusual transaction sequences
- Velocity checks on deposit frequency and amounts
- Cross-referencing payment methods to identify third-party funding
- Monitoring for minimal gaming activity relative to deposits (pass-through transactions)
- Detection of multiple accounts linked by shared identifiers (IP, device, payment method)

Automated alerts are reviewed by the compliance team within 24 hours. All reviews and decisions are documented.

7.0 Suspicious Activity Reporting

Internal Reporting: All staff must report any suspicion of money laundering or terrorism financing to the MLRO immediately. Reports can be made via the internal reporting system, email, or in person. Staff are protected from retaliation for making good-faith reports.

External Reporting: The MLRO evaluates all internal reports and, where appropriate, files Suspicious Activity Reports (SARs) / Unusual Transaction Reports (UTRs) with the Financial Intelligence Unit of Curaçao (FIU) within the prescribed timeframe.

Tipping Off: It is strictly prohibited to disclose to a customer or any third party that a SAR/UTR has been filed or that an investigation is underway. Breach of tipping-off provisions may result in criminal prosecution and immediate dismissal.

8.0 PEP & Sanctions Screening

All customers are screened against:

- PEP databases (domestic and international)

- UN Security Council Consolidated Sanctions List
- EU Consolidated Sanctions List
- OFAC Specially Designated Nationals (SDN) List
- Local Curaçao sanctions and watchlists
- Adverse media databases

Screening is performed at account registration, at regular intervals (ongoing monitoring), and upon any change in customer information. Matches are reviewed by the compliance team and escalated to the MLRO for decision.

9.0 Record Keeping

The operator maintains records in accordance with CGA requirements and applicable legislation:

- Customer identification and verification documents — retained for minimum 5 years after account closure
- Transaction records (deposits, withdrawals, wagering) — retained for minimum 5 years
- SAR/UTR records and related documentation — retained for minimum 5 years after filing
- Risk assessments and compliance reports — retained for minimum 5 years
- Training records — retained for duration of employment plus 5 years

All records are stored securely with appropriate access controls and are available for inspection by the CGA and other competent authorities upon request.

10.0 Staff Training

All employees receive AML/CFT training:

- **Induction Training:** Mandatory AML/CFT awareness training before commencing duties
- **Annual Refresher:** All staff complete annual AML/CFT refresher training
- **Role-Specific Training:** Enhanced training for compliance, finance, and customer-facing staff
- **Regulatory Updates:** Ad-hoc training when significant regulatory changes occur

Training records are maintained and submitted to CGA upon request. Training effectiveness is assessed through testing and practical scenarios.

11.0 Governance & MLRO

Money Laundering Reporting Officer (MLRO): A senior, qualified individual appointed as MLRO with:

- Direct access to Board of Directors
- Authority to suspend accounts and freeze funds pending investigation
- Responsibility for SAR/UTR filing with FIU
- Oversight of the AML/CFT compliance program
- Reporting to CGA as required

Board Responsibility: The Board of Directors has ultimate responsibility for AML/CFT compliance. The Board receives regular reports from the MLRO and approves the AML policy and risk assessment.

12.0 Policy Review & Updates

This policy is reviewed at least annually, or more frequently in response to:

- Changes in CGA regulations or guidance
- Changes in FATF recommendations or national legislation
- Findings from internal or external audits
- Significant changes to business operations, products, or markets
- Identified deficiencies in AML/CFT controls

All policy changes are approved by the MLRO and Board of Directors, communicated to all staff, and reported to the CGA as required.