

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

IBC BROKER B.V.

License Number: OGL/2024/1230/1099

Company Number: 148161

Registered Address: Abraham Mendez Chumaceiro Boulevard 03, Curaçao

Websites: www.bet-ibc.com | www.vip-ibc.com | www.betspider.com |

www.bettingsoftware.com

1. Policy Statement

IBC BROKER B.V. acknowledges its responsibility to implement and maintain robust systems to prevent money laundering (ML), terrorist financing (TF), and proliferation financing. This policy represents the company's unwavering commitment to integrity, transparency, and compliance with the Curaçao Gaming Control Board (GCB) regulations, National Ordinance on Games of Chance (LOK), Curaçao AML/CFT/CPF laws (including NOIS, NORUT, Sanctions National Ordinance, and Kingdom Sanctions Act), FATF Recommendations, and EU AML Directives (where applicable). It applies across all operations, including customer onboarding, payment processing, player support, and risk monitoring. All employees, partners, and affiliates must adhere strictly to this policy. The company adopts a risk-based approach, ensuring measures are proportionate to identified risks.

2. Purpose

The primary purpose of this policy is to establish a structured framework that safeguards IBC BROKER B.V. from being misused for illicit financial activities. It ensures compliance with:

- Curaçao National Ordinance on Games of Chance (LOK)
- Curaçao AML/CTF regulations (NOIS, NORUT, Sanctions National Ordinance, Kingdom Sanctions Act)
- FATF recommendations
- EU AML Directives (where applicable)

By enforcing strict procedures, this policy protects the company's reputation, regulatory license, and financial ecosystem while ensuring safe and transparent operations.

This policy applies to all operations, including customer onboarding, payment processing, transaction monitoring, player support, affiliate management, and third-party relationships. All directors, officers, employees, contractors, and business partners must comply fully with this policy.

3. Audience

This policy is mandatory for:

- All IBC BROKER B.V. employees, directors, and officers
- Contractors, suppliers, and affiliates
- Third-party KYC/AML service providers
- Customer support staff, risk analysts, and compliance personnel

Non-compliance by any party will lead to disciplinary action, contract termination, or regulatory escalation.

4. Definitions

The following terms apply throughout this policy:

Money Laundering (ML): Concealing the origins of illicit funds.

Terrorist Financing (TF): Providing financial support to terrorism-related activities.

Anti-Money Laundering (AML): Measures to prevent criminals from disguising illegally obtained funds as legitimate income.

Beneficial Owner (UBO): The natural person(s) who ultimately own or control a customer, or on whose behalf a transaction is conducted (typically 25%+ ownership or control).

Business Relationship: Any professional or commercial relationship between IBC BROKER and a customer that has an element of duration (i.e., account-based relationship).

Cash Equivalent: Cashless transactions, prepaid cards, cryptocurrency, or other anonymous payment methods.

Counter-Terrorist Financing (CTF): Measures to prevent the provision of funds or financial services for terrorist activities.

Counter-Proliferation Financing (CPF): Measures to prevent financing of weapons of mass destruction.

Customer Due Diligence (CDD): The process of identifying and verifying customer identity, understanding business relationships, and ongoing monitoring.

Customer Risk Assessment (CRA): Risk evaluation of individual customers based on jurisdiction, occupation, source of funds, transaction patterns, and other factors.

Enhanced Due Diligence (EDD): Additional scrutiny applied to higher-risk customers or transactions.

Financial Intelligence Unit (FIU): Curaçao's authority responsible for receiving, analyzing, and disseminating suspicious transaction reports.

Financial Transaction: For online casinos, deposits and withdrawals (excluding bonuses). Wagering and winnings are gambling transactions, not financial transactions.

Occasional Transaction: A one-time transaction with a customer not expected to return (typically in land-based contexts).

Ongoing Monitoring: Continuous scrutiny of customer transactions and account activity to detect unusual patterns.

Politically Exposed Person (PEP):

- **Foreign PEPs:** Individuals entrusted with prominent public functions in a foreign country
- **Domestic PEPs:** Individuals entrusted with prominent public functions in Curaçao

- **International Organization PEPs:** Senior management of international organizations
- Includes family members and close associates

Simplified Due Diligence (SDD): Reduced CDD measures for lower-risk customers (subject to restrictions).

Source of Funds (SOF): The origin of funds for a specific transaction (e.g., salary, property sale, inheritance).

Source of Wealth (SOW): The origin of a customer's total accumulated wealth (e.g., employment, business ownership, investments).

Suspicious Transaction Report (STR): Also called Unusual Transaction Report (UTR); a report filed with the FIU regarding transactions suspected of ML/TF/FP.

Targeted Financial Sanctions: Mandatory freezing of funds/assets of designated persons or entities under UN/EU sanctions.

Tipping Off: Unlawfully disclosing to a customer or third party that a suspicious transaction report has been filed or is being considered.

Unusual Transaction: A transaction considered suspicious based on objective or subjective indicators under NORUT.

5. Policy Implementation

Implementation of this AML/CFT policy requires a comprehensive governance structure, specialized compliance team, and advanced technological solutions. Key components include:

- Governance: Oversight by the Compliance Officer and Board of Directors.
- Risk-based approach: All procedures are proportional to the risks identified.
- Technology: Automated transaction monitoring, sanctions screening, and fraud detection systems.
- Human oversight: Manual reviews, staff reporting, and escalation procedures.
- Training: Regular training for all relevant staff.

Implementation ensures that preventive and detective measures are aligned with regulatory requirements.

5.1 Business Risk Assessment

IBC BROKER B.V. conducts an annual business risk assessment covering:

- Geographic exposure: Countries where customers reside.
- Payment channels: Bank transfers, e-wallets, cryptocurrencies.
- Products and services: Betting, exchanges, and software tools.
- Customer base: Retail players, agents, affiliates.

The assessment identifies vulnerabilities and ensures adequate controls are in place. Results are reported to senior management and used to enhance policies.

Scope of Business Risk Assessment (BRA):

1. Customer Risk Factors:

- Geographic distribution of customers
- Customer types (retail, VIP, agents, affiliates)

- PEP exposure
- High-value/high-frequency customers
- Multiple accounts or unusual patterns
- 2. **Geographic Risk Factors:**
 - Countries with weak AML/CFT frameworks (FATF/CFATF lists)
 - High-risk jurisdictions (sanctions, corruption, terrorism)
 - Source of customer base by country
 - Sources consulted: FATF High-Risk Jurisdictions, CFATF Public Statements, Transparency International Corruption Index, OFAC sanctions lists
- 3. **Product, Service, and Transaction Risk:**
 - Payment methods accepted (cards, e-wallets, cryptocurrency, bank transfers)
 - Anonymous payment methods (prepaid cards, virtual assets)
 - Betting products and services (sports betting, exchanges)
 - Risk of proceeds of crime, fraud, or identity theft
 - Peer-to-peer gaming products
 - Multiple platform/wallet usage
- 4. **Distribution Channel Risk:**
 - Online platforms (non-face-to-face interaction)
 - Use of agents or affiliates
 - Physical establishments (if applicable)
 - Third-party payment processors

Methodology:

- Risk factors categorized as low, medium, or high
- Documented rationale for each risk rating
- Considers National Risk Assessment outcomes for Curaçao and operational jurisdictions
- Approved by Board of Directors
- Made available to GCB upon request

Outcome: The BRA informs our risk appetite, customer acceptance criteria, and resource allocation for AML/CFT controls.

5.2 Customer Risk Assessment

Each customer is assigned a risk rating (low, medium, high) based on:

Risk Factors Considered:

1. **Customer Profile:**
 - Nationality and country of residence
 - Occupation and income sources
 - Age and identification verification quality
 - PEP status or sanctions exposure
2. **Transactional Behavior:**
 - Deposit frequency and amounts

- Withdrawal patterns
 - Rapid cycling of funds (deposit/withdrawal without play)
 - Use of third-party payment accounts
 - Discrepancies between stated income and transaction volume
3. **Geographic Risk:**
- Residence in high-risk jurisdictions
 - Use of payment methods from high-risk countries
 - IP address inconsistencies
4. **Source of Funds/Wealth:**
- Clarity and verifiability of stated sources
 - Consistency with expected profile
 - Documentation quality

Risk Rating Determines CDD Level:

- **Low Risk:** Simplified Due Diligence (where permitted)
- **Medium Risk:** Standard Due Diligence
- **High Risk:** Enhanced Due Diligence

Risk ratings are reviewed periodically and updated when material changes occur (e.g., transaction pattern changes, adverse media, PEP identification).

5.3 Customer Acceptance Policy

IBC BROKER B.V. enforces a strict Customer Acceptance Policy (CAP). Customers will not be accepted if:

- They fail identity verification.
- They appear on sanctions or PEP watchlists without proper clearance.
- Their source of funds cannot be established.
- They are minors or restricted by law.

The CAP ensures that only legitimate players access company platforms.

5.4 Customer Due Diligence

CDD measures include:

- Collection of government-issued identification documents.
- Proof of residence (utility bill, bank statement).
- Verification of payment methods.
- PEP and sanctions screening.
- Ongoing transaction monitoring.

Enhanced Due Diligence (EDD) applies for high-risk customers, including:

- Detailed source of wealth/funds checks.
- Senior management approval before account activation.
- Increased monitoring and transaction review.

If suspicion arises, funds are frozen, and an STR is filed with the FIU.

5.4.1 CDD Triggers

CDD measures are required when:

- a) A customer engages in financial transactions (deposits/withdrawals) equal to or above **NAf 4,000 (approx. 1,900 EUR)** (cumulative daily total)
- b) Carrying out occasional transactions above NAf 4,000
- c) There is suspicion of money laundering, terrorist financing, or proliferation financing
- d) Doubts exist about previously obtained customer identification data

Linked Transactions: A series of transactions by the same customer through the same game or gaming session that cumulatively reach NAf 4,000 are treated as a single transaction for CDD purposes.

5.4.2 Timing of CDD Measures

At Account Opening (Minimum CDD):

- Full name
- Permanent residential address
- Date of birth
- PEP status screening
- Sanctions screening (UN, EU, Curaçao lists)
- Customer declaration of transacting on own behalf

When NAf 4,000 Threshold Reached:

- Complete identity verification using government-issued ID (passport, national ID card)
- Proof of address verification (utility bill, bank statement dated within 6 months)
- Customer Risk Assessment
- Additional information as required by risk rating
- Complete CDD must be finalized within **30 days** of threshold being reached

Failure to Complete CDD: If required documentation is not received within 30 days:

1. Account is suspended (deposits and withdrawals blocked)
2. If no suspicion of ML/TF exists: funds returned to source account/wallet
3. If suspicion of ML/TF exists: Suspicious Transaction Report filed with FIU; account frozen pending FIU guidance
4. Relationship terminated.

5.4.3 Standard CDD Measures

a) Identification of the Customer

Minimum information collected:

1. Full legal name (as per government ID)
2. Permanent residential address
3. Date of birth
4. Place of birth
5. Nationality
6. Identity document number and issuing authority

Low-risk customers: May be limited to name, address, and date of birth initially.

High-risk customers: Additional information required (occupation, employer, income sources, previous addresses).

b) Verification of Identity

Acceptable documents:

- Unexpired government-issued photo ID (passport, national ID card, driver's license)
- Proof of address (utility bill, bank statement, government letter, rental agreement) dated within **6 months**

Verification methods:

- Document authentication (check for tampering, validity)
- Biometric verification (selfie with ID, liveness detection)
- Cross-reference with reliable databases
- Email/phone verification
- Geo-location and IP address analysis
- Payment method verification (account holder name matching)

For unfamiliar foreign documents, extra authentication measures are applied.

c) Sanctions and PEP Screening

All customers screened against:

- UN Security Council Consolidated Sanctions List
- EU Sanctions Map
- Curaçao local sanctions lists (if published)
- PEP databases (international and domestic)
- Adverse media sources

Screening performed:

- At account opening
- When NAf 4,000 threshold reached
- Periodically during relationship (at least annually for medium/high-risk customers)
- Upon regulatory list updates

d) Beneficial Owner Identification

Applies when:

- Corporate accounts are opened
- Customer is acting on behalf of third parties (syndicates, groups)
- Use of physical establishments or agent structures

For beneficial owners:

- Identify all natural persons holding 25%+ ownership or control
- Obtain same identification/verification as for customers
- If no person meets threshold: identify senior managing official

e) Purpose and Intended Nature of Business Relationship

Understanding why the customer is using our services and expected activity levels.

Information collected (risk-based):

- Occupation and employment details
- Nature of business (if self-employed)
- Expected deposit frequency and amounts
- Source of funds for gambling activity
- Source of wealth (high-risk customers only)

Low-risk: Customer declaration with basic details (employment, income range)

Medium-risk: Supporting documentation (payslips, bank statements)

High-risk: Independent verification of SOW/SOF (employer verification, tax documents, property records)

Statistical Profiling (where applicable): For established customer bases, average wagering profiles may be used to detect deviations. Not applicable for high-risk customers or new operations without sufficient data.

f) Ongoing Monitoring

Transaction Monitoring:

- Automated systems flag unusual patterns:
 - Deposits/withdrawals exceeding customer profile
 - Rapid deposit/withdrawal cycles (minimal play)
 - Transactions inconsistent with stated occupation/income
 - Use of multiple accounts or payment methods
 - High-risk jurisdiction transactions
 - Structured transactions (just below reporting thresholds)

Identity Monitoring:

- Periodic refresh of identification documents (especially upon expiry)
- Re-verification triggered by key events (payment method changes, address changes, large transactions)
- Ongoing PEP/sanctions screening

Risk Re-Assessment: Customer risk ratings reviewed:

- Upon significant transactional changes
- Annually for medium/high-risk customers
- When adverse information is discovered
- Upon regulatory or business changes

5.4.4 Enhanced Due Diligence (EDD)

Applied to higher-risk customers, including:

1. **Foreign PEPs** (mandatory)
2. **Domestic PEPs and International Organization PEPs** (if high-risk)
3. Customers from high-risk jurisdictions (FATF/CFATF lists)
4. Customers using high-risk payment methods (cryptocurrency, anonymous prepaid cards)
5. Customers with unusual transaction patterns
6. Customers with adverse media exposure
7. High-value customers (deposits exceeding €10,000 per month)
8. New products/technologies with heightened risk

EDD Measures:

- Obtain additional identification documents
- Senior management approval required (by Compliance Officer or Director)
- Establish and verify source of wealth (employment history, business ownership, inheritance, investments)

- Establish and verify source of funds for specific transactions (recent payslips, sale contracts, bank statements)
- Obtain additional information on purpose of relationship
- Increased frequency and intensity of ongoing monitoring
- Periodic SOW/SOF reviews (at least annually)
- First payment required from account in customer's name held at reputable financial institution

For PEPs:

- Source of wealth and source of funds must be established and verified
- Senior management approval mandatory
- Enhanced ongoing monitoring mandatory
- Measures also apply to family members and close associates

5.4.5 Simplified Due Diligence (SDD)

Applied only where ML/TF risk is demonstrably low.

Permitted measures:

- Limit initial identification to name, address, date of birth
- Reduce verification requirements (alternative information sources)
- Reduce frequency of identity updates
- Reduce intensity of transaction monitoring (with risk-appropriate thresholds)

Restrictions:

- SDD **not permitted** when suspicion of ML/TF exists
- SDD **not permitted** for high-risk scenarios (PEPs, high-risk jurisdictions, anonymous payments)

5.4.6 Existing Customers

For customers onboarded before April 10, 2025:

- Apply CDD measures on a risk-sensitive basis
- Prioritize high-risk customers for immediate review
- Complete CDD when next significant transaction occurs or by **October 10, 2025**, whichever is sooner
- Ongoing monitoring standards apply immediately

5.5 Ongoing Monitoring

Transaction Monitoring.

All customer accounts are monitored for unusual activity. Monitoring tools detect:

- Large or rapid transactions inconsistent with profile.
- Frequent deposits and withdrawals without clear purpose.
- Attempts to bypass deposit limits.
- Transactions with high-risk jurisdictions.

Flagged transactions are escalated to the Compliance Officer.

Alert Review Process:

1. System generates alert

2. Compliance team reviews transaction details, customer profile, and history
3. If suspicious: escalate to Compliance Officer
4. If explanation required: contact customer for clarification (unless tipping-off risk exists)
5. Document outcome (cleared or reported to FIU)

Frequency:

- Real-time monitoring for high-risk customers
- Daily batch monitoring for medium-risk customers
- Weekly monitoring for low-risk customers

5.6 Reliance on Third Parties

IBC BROKER B.V. may engage licensed third-party KYC/AML service providers. When doing so:

- A written agreement is in place.
- The provider must comply with Curaçao AML laws.
- IBC retains full responsibility for compliance.

Outsourcing does not remove the company's accountability.

5.7 Reporting of Unusual Transactions

Employees must immediately escalate suspicious transactions to the Compliance Officer. The Compliance Officer evaluates and, if appropriate, submits a Suspicious Transaction Report (STR) to the FIU. Examples of unusual transactions:

- Multiple large deposits with no clear purpose.
- Players refusing to provide KYC documents.
- Sudden changes in betting patterns.
- Use of multiple accounts or third-party payments.

Non-reporting by staff is a violation of this policy.

5.7.1 Objective Indicators (Mandatory Reporting - NAf 5,000+ Threshold):

Per Ministerial Decree (N.G. 2015 no. 73), the following transactions of NAf 5,000 or more must be reported to the FIU:

1. Cashless transactions (bank transfers) of NAf 5,000+
2. Accepting or releasing deposits of NAf 5,000+
3. Sale of chips/tokens/credits of NAf 5,000+
4. Cash-outs of NAf 5,000+
5. Credit card transactions of NAf 5,000+
6. E-wallet transactions of NAf 5,000+

Note: Threshold calculated per gaming day. A series, combination, or pattern of transactions totaling NAf 5,000+ is reportable.

Subjective Indicators (Suspicion-Based Reporting):

Transactions reported when there is cause to presume ML/TF/FP, including:

- Customer refuses or delays providing CDD documents

- Customer provides false or inconsistent information
- Use of multiple accounts to avoid thresholds
- Transactions inconsistent with customer profile (occupation, income)
- Rapid deposit/withdrawal with minimal or no play
- Unusual betting patterns (e.g., betting on all outcomes)
- Use of third-party payment accounts
- Transactions involving high-risk jurisdictions
- Customer appears on adverse media or sanctions lists
- Transactions following tips from law enforcement or FIU
- Structuring (breaking transactions to avoid reporting)
- Customer requests anonymity or excessive secrecy
- Transactions with no apparent economic purpose

Additional Reportable Situations:

- a) Transactions reported to Police or Department of Justice in connection with ML/TF
- b) Transactions by or on behalf of persons named on UN/EU/Curaçao sanctions lists
- c) Attempted transactions that are declined due to ML/TF suspicion

5.7.2 Internal Reporting Procedure

1. **Detection:** Employees, automated systems, or compliance reviews detect unusual activity
2. **Escalation:** Employee immediately reports to Compliance Officer via internal reporting form
3. **Documentation:** All supporting documents attached (transaction records, CDD documents, communications, screenshots)
4. **Assessment:** Compliance Officer reviews within 24 hours
5. **Decision:** Compliance Officer determines if external report to FIU required
6. **Record-Keeping:** If not reported to FIU, rationale documented and signed by Compliance Officer

Internal Reporting Form Includes:

- Customer name, account ID, registration date
- Transaction details (date, amount, payment method, description)
- Reason for suspicion (indicator triggered)
- Supporting evidence
- Employee name and date of report

5.7.3 External Reporting to FIU

Timing: Unusual transactions reported to FIU **without delay** (immediately upon determination).

Method: Via FIU's goAML reporting portal.

Report Contents:

- Customer identification details
- Transaction details (date, amount, method, currency)
- Reason for suspicion (indicators)

- Supporting documentation (ID copies, transaction records, correspondence)
- Report in English language

5.8. Targeted Financial Sanctions and Freezing Procedures

5.8.1 Sanctions Screening

All customers screened against:

- UN Security Council Consolidated Sanctions List
- EU Sanctions Map (all regimes)
- Curaçao local sanctions lists (if published)
- OFAC Specially Designated Nationals (SDN) List (for US-connected transactions)

Screening Timing:

- At account registration
- Upon NAF 4,000 threshold
- When sanctions lists are updated (immediate re-screening)
- Periodically during relationship (at least monthly for existing customers)

Screening Sources:

- <https://main.un.org/securitycouncil/en/content/un-sc-consolidated-list>
- <http://www.sanctionsmap.eu/>
- GCB website for Curaçao updates

IBC BROKER monitors GCB website and regulatory announcements for sanctions updates.

5.8.2 Freezing of Funds Procedure

If Sanctions Match Identified:

1. Immediate Action:

- Freeze account immediately (block all deposits, withdrawals, and gameplay)
- Do not notify customer (to avoid tipping off)
- Escalate to Compliance Officer immediately

2. Verification:

- Compliance Officer verifies match (name, DOB, nationality, aliases)
- Consider false positives (common names)
- Document verification process

3. Reporting:

- File Unusual Transaction Report with FIU immediately
- Report to Curaçao Ministry of Justice (as per Process for Freezing of Resources, N.G. 2016)
- Include: customer details, account balance, transaction history, reason for freeze

4. Awaiting Guidance:

- Maintain freeze until instructed by FIU or Ministry of Justice
- Do not release any funds
- Provide additional information upon request

5. Record-Keeping:

- Document all actions taken

- Maintain records of frozen accounts separately
- Report frozen assets in annual compliance reports to GCB

No Prior Notice Rule: Freezing must occur **without prior notice** to the customer to comply with UN/EU requirements.

5.9 Technological Developments Risk Assessment

Before launching new products, services, delivery mechanisms, or technologies, IBC BROKER conducts a risk assessment to identify ML/TF/FP vulnerabilities.

Assessment Scope:

- New payment methods (e.g., new cryptocurrency, e-wallet providers)
- New betting products or markets
- New technologies (e.g., blockchain-based gaming, NFTs)
- New business practices (e.g., affiliate models, bonus structures)
- New customer interfaces (e.g., mobile apps, API integrations)

Assessment Process:

1. Identify innovation and describe functionality
2. Analyze potential ML/TF/FP risks (anonymity, cross-border, rapid transactions)
3. Identify existing controls and gaps
4. Design mitigation measures (enhanced CDD, transaction limits, monitoring rules)
5. Document assessment and obtain senior management approval
6. Implement controls before launch
7. Review effectiveness post-launch

Documentation retained and provided to GCB upon request.

5.10 Termination of Business Relationship

IBC BROKER will terminate a customer relationship when:

1. Customer fails to provide required CDD documentation within 30 days of NAF 4,000 threshold
2. Customer fails identity verification
3. Customer identified on sanctions lists
4. Customer is a PEP and required approvals/EDD not completed within 30 days
5. Customer provides false or misleading information
6. Suspicion of ML/TF/FP exists and continuing relationship poses unacceptable risk
7. Customer engages in prohibited activities (fraud, bonus abuse, underage gambling)
8. Ongoing monitoring reveals unacceptable risk

Termination Procedure:

If No Suspicion of ML/TF:

1. Notify customer of account closure (generic reason)
2. Return funds to source account/wallet (same channel as deposit)
3. Document reason for termination
4. Retain records for 5 years after termination

If Suspicion of ML/TF Exists:

1. Do not notify customer (tipping-off risk)

2. Freeze account immediately
3. File Suspicious Transaction Report with FIU
4. Await FIU guidance on fund disposition
5. Consider whether account blocking itself may tip off customer; if so, increase monitoring instead and file ongoing STRs
6. Document all actions

Fund Return: Funds returned only via same method used for deposit. If deposit method unavailable or suspicious, await FIU instructions.

Record of Termination:

- Customer details
- Date of termination
- Reason (documented in detail for internal records)
- Actions taken (notifications, fund returns, reports filed)
- Signed by Compliance Officer

5.11 AML Compliance Program

The compliance program includes:

- Appointment of a dedicated Compliance Officer (Mihaela Prida).
- Independent internal audits and regular CGA reporting.
- Comprehensive record-keeping (minimum five years).
- Transaction monitoring and escalation systems.
- Procedures for blocking suspicious accounts immediately.

The program is reviewed annually and updated as needed.

6. Compliance and Consequences of Non-Compliance

Non-compliance with this policy can result in:

- Disciplinary action, including termination of staff.
- Contract suspension for third-party providers.
- Regulatory fines, penalties, or license revocation.
- Criminal liability where laws are breached.

All breaches are reported to management and regulators.

7. Related Information

This policy must be interpreted alongside:

- Responsible Gaming Policy (2025)
- Player Complaints Policy (2025)
- Terms and Conditions
- Data Privacy and Protection Policy
- Curaçao AML/CTF laws and FATF guidelines

8. Contact Information

For compliance-related questions or to report suspicious activity:

Compliance Officer: Ana Prutean

Email: compliance@ibcbroker.org

Director: Patrick Edmond Monnissen

9. Policy History

Version 1.0 – Effective Date: 10 December 2025

Initial release of AML/CFT Policy for IBC BROKER B.V.

Reviewed annually by Compliance Department and Board of Directors.

10. Policy URL

This policy will be published on all operational websites:

- www.bet-ibc.com
- www.vip-ibc.com
- www.betspider.com
- www.bettingsoftware.com

11. Signature and Validation

Signed on behalf of IBC BROKER B.V.

Patrick Edmond Monnissen

Director

IBC BROKER B.V.

Date: 10 December 2025

DocuSigned by:
Patrick Edmond Monnissen
AC11EE5A13FF4F1...