AML & CTF Policy

BitVegas.gg | Version 1.0 | Effective Date: 14 August 2026

Operated by Blockdance S.R.L., including its subsidiaries and affiliates, 300 Este de la Iglesia Católica, Granadilla, Curridabat, San José, Costa Rica (the “Operator”, “we”, “us”, “our”).

This Anti-Money Laundering and Counter-Terrorist Financing Policy (the “Policy”) sets out the framework applied by the Operator of bitvegas.gg to prevent the Platform from being used for money laundering, terrorist financing, sanctions evasion, fraud, or other financial crime. This Policy forms part of the Terms & Conditions and is binding on all account holders.

1. Commitment and Legal Framework

1.1 The Operator maintains a risk-based AML/CTF program aligned with the recommendations of the Financial Action Task Force (FATF), the conditions of its gaming license, and applicable anti-money-laundering legislation.

1.2 The program is overseen by a designated Money Laundering Reporting Officer (“MLRO”) with authority to suspend accounts and transactions, file reports with competent authorities, and direct investigations.

2. Risk-Based Approach

2.1 Each customer and transaction is assessed against risk factors including: geographic risk (jurisdiction of residence and of funds), product risk, transaction size, velocity and pattern, deposit-to-wagering ratio, use of multiple assets or wallets, and behavioral indicators.

2.2 Customers are assigned a risk rating (standard, elevated, high) which determines the intensity of due diligence and monitoring applied. Risk ratings are reviewed on trigger events and periodically.

3. Customer Due Diligence (CDD)

3.1 CDD is applied on registration and throughout the customer relationship, and includes collection and verification of identity data as described in the KYC & Verification Policy.

3.2 Verification is mandatory, without limitation, where: (a) cumulative deposits or withdrawals reach $2,000 (USD equivalent) or such lower threshold as the Operator applies; (b) a withdrawal is requested; (c) risk indicators are present; (d) required by the MLRO or by law. The Operator may apply verification at any lower threshold at its discretion.

3.3 Enhanced Due Diligence (EDD) — including source-of-funds (SoF) and source-of-wealth (SoW) evidence — applies to high-risk customers, politically exposed persons (PEPs), large or unusual transaction activity, and cumulative activity exceeding $10,000 (USD equivalent), or on any trigger determined by the MLRO.

3.4 The Operator does not open or maintain anonymous accounts and does not deal with shell entities. Business is refused or terminated where CDD cannot be completed.

4. Sanctions and PEP Screening

4.1 Customers are screened against applicable sanctions lists (including UN, OFAC, EU, and UK lists) and PEP databases at onboarding and on an ongoing basis. Confirmed sanctions matches result in immediate account freezing and reporting as required by law.

5. Cryptocurrency-Specific Controls

5.1 Deposits and withdrawals are monitored using blockchain analytics. The Operator may reject or return funds associated with: mixers and tumblers, darknet markets, sanctioned wallets, ransomware, stolen funds, high-risk exchanges, or wallets with no verifiable transaction history commensurate with the customer's profile.

5.2 Privacy-enhanced transfer methods that defeat traceability are not accepted. The Operator may require proof of wallet ownership (e.g., signed message or satoshi test) at any time.

5.3 Third-party funding is prohibited: deposits must come from wallets owned and controlled by the account holder, and withdrawals are made only to the account holder.

6. Transaction Monitoring

6.1 Automated and manual monitoring is applied to detect red flags including: deposits withdrawn with minimal or no wagering ("pass-through" activity), structuring below thresholds, rapid movement between assets, mismatches between activity and customer profile, shared devices or wallets across accounts, and wagering patterns designed to transfer value between accounts (chip dumping).

6.2 Every deposit must be wagered at least once (1x) before withdrawal. The Operator may delay, decline, or reverse any transaction pending review and may return funds to their originating address.

7. Reporting

7.1 Suspicious activity is escalated internally to the MLRO, who determines whether a suspicious activity/transaction report must be filed with the competent authority. Where a report is filed or under consideration, the Operator may freeze funds and is prohibited from disclosing the report to the customer ("tipping off").

8. Record Keeping

8.1 CDD records, transaction records, game logs, and analysis are retained for a minimum of five (5) years after the end of the customer relationship or the transaction date, whichever is later, or such longer period as required by law.

9. Training and Audit

9.1 Relevant staff receive AML/CTF training at onboarding and at least annually. The program is subject to periodic independent review, and this Policy is reviewed at least annually by the MLRO.

10. Customer Obligations

10.1 By using the Platform you agree to: provide truthful information and documents promptly on request; use only funds of lawful origin that belong to you; and refrain from any activity described in this Policy. Breach may result in voided winnings, account closure, retention of funds where legally required, and reporting to authorities.