AML & KYC Policy

HighBinary Technologies Ltd | Version 1.1 | Revised 25 November 2026

Application: this revision takes effect upon authorised publication and any notice or acceptance required by applicable law.

Anti-Money Laundering & Know Your Customer Policy

01 / Purpose and scope

This Anti-Money Laundering and Know Your Customer Policy (AML & KYC Policy) sets out the principles governing identity verification, financial crime prevention and transaction review on HighBinary, operated by HighBinary Technologies Ltd (the Company). It applies to applicants, account holders and relevant payment activity. It must be read with the Terms & Conditions and Privacy Policy. Applicable mandatory law prevails over this Policy.

02 / Financial crime prevention

The Company prohibits use of its services for money laundering, terrorist financing, proliferation financing, fraud, sanctions evasion or other unlawful activity. The Company shall apply proportionate, risk-based controls and maintain appropriate internal procedures, oversight and escalation arrangements as required by applicable law. This Policy does not constitute a statement of regulatory authorisation.

03 / Eligibility and account ownership

Users must be at least 18 years old, or older where local law requires, and legally eligible to use the services in their jurisdiction. Each user may maintain one main account and must act on their own behalf. False identities, impersonation, undisclosed third-party control and attempts to circumvent geographic or account restrictions are prohibited. Users must provide accurate information and promptly report material changes.

04 / Timing of identity verification

Verification may be required at registration, before access to particular services, before deposits or withdrawals, during periodic reviews or when security or financial crime concerns arise. Where law requires verification before establishing a relationship or carrying out a transaction, the Company shall not defer that verification. Access may be limited until required checks are completed.

05 / Identity and supporting documents

The Company may request a valid passport, national identity card or driving licence, a selfie or other identity confirmation, and, where proportionate, evidence of residential address, date of birth, nationality or payment ownership. Documents must be authentic, legible and current. Additional information may be requested where evidence is inconsistent or insufficient. Verification may involve automated checks and manual review.

06 / Risk assessment and ongoing due diligence

The Company shall assess relevant risk factors, including location, account activity, transaction patterns, payment methods, identity inconsistencies and applicable sanctions exposure. Reviews may be repeated when circumstances change or information becomes outdated. Controls shall be proportionate to identified risk and applicable legal obligations; no single risk factor necessarily establishes wrongdoing.

07 / Enhanced due diligence

Higher-risk cases may require additional identity evidence, explanations of transaction purpose, source of funds or source of wealth, and additional review or approval before services continue. Politically exposed persons, their family members and known close associates shall be assessed in accordance with applicable law. Such status alone does not establish criminal conduct or automatically justify rejection.

08 / Source of funds and source of wealth

Where justified by risk or law, users may be asked to explain how funds used on the platform were obtained and, where relevant, how their overall wealth was accumulated. Supporting evidence may include bank statements, employment income records, business records, sale agreements or other reliable documentation. Requests shall be limited to information reasonably necessary for the review.

09 / Sanctions and geographic restrictions

The Company shall comply with applicable sanctions and restrictions and may screen users, relevant counterparties and transactions against applicable lists. Potential matches shall be assessed before a determination is made, subject to legal requirements. Services must not be provided where prohibited. Users must not conceal their location or use intermediaries to evade lawful restrictions.

10 / Deposits and payment ownership

Deposits must originate from lawful sources and payment methods owned or lawfully controlled by the user. Third-party funding is not permitted unless expressly lawful and authorised under applicable service rules. The Company may request evidence of payment ownership, investigate disputed payments and reject or return funds where lawful. No payment method may be used to disguise the origin of funds.

11 / Withdrawals and payment verification

Withdrawals may be made through supported methods different from the deposit method, subject to verification, available funds, limits and legal requirements. Withdrawal destinations must belong to the user or be demonstrably under their authorised control. Payments to unrelated third parties are prohibited; mandatory lawful refunds to the original payment source or legally required payment directions are handled separately under applicable law. Additional checks may delay processing. Where lawful and practicable, the Company communicates status and requested information.

12 / Digital assets and blockchain transactions

Where cryptocurrency payments are supported, the Company may assess wallet ownership, transaction history and exposure to illicit or sanctioned activity using proportionate checks. Users may be asked to provide transaction identifiers or evidence of wallet control. Blockchain transfers may be irreversible. Additional restrictions or information requirements may apply under applicable digital asset and transfer rules.

13 / Transaction monitoring and suspicious activity

The Company shall apply risk-based review of transactions and account activity. Unusual patterns may include unexplained rapid movement of funds, inconsistent payment ownership, suspected identity misuse, repeated attempts to bypass controls or activity inconsistent with known account information. Indicators trigger assessment and do not by themselves establish wrongdoing. Users must cooperate with lawful and proportionate enquiries.

14 / Restrictions, investigations and reporting

Where justified by risk or required by law, the Company may delay, decline or restrict transactions, suspend access or terminate a relationship following appropriate review. The Company shall report suspicious activity to competent authorities where legally required and comply with lawful orders. Information may be withheld where disclosure is prohibited, including applicable restrictions on tipping off.

15 / Handling of funds and account closure

Restrictions shall not automatically result in forfeiture of user funds. Funds shall be handled in accordance with applicable law, lawful orders and the Terms & Conditions. Where permitted, verified funds shall be returned through an appropriate verified payment route after necessary checks. The Company shall not release funds in breach of sanctions, freezing orders or other legal restrictions.

16 / Privacy, security and retention

Identity documents, verification results and transaction records shall be processed for legitimate and lawful purposes under the Privacy Policy. Access shall be restricted to authorised personnel and service providers as necessary. Records shall be retained for periods required by applicable law or justified by lawful purposes, then securely deleted or anonymised where appropriate. Legal retention obligations may limit deletion requests.

17 / Service providers and internal governance

The Company may use identity verification, payment processing, blockchain analysis or other specialist providers subject to appropriate due diligence, confidentiality and data protection arrangements. The Company remains responsible for its own applicable obligations. Relevant personnel shall receive appropriate guidance and training; controls shall be reviewed and updated in response to changing risks and legal requirements.

18 / User rights, complaints and review

Users may request clarification or challenge verification or restrictions through Contact Support or support@highbinarytrading.com. Where applicable, users may request human review of automated decisions and exercise data protection rights. Complaints are assessed fairly and outcomes communicated where lawful. Mandatory rights remain available.

19 / Updates and user cooperation

Users must cooperate with lawful verification requests and keep their account information accurate. The Company may update this Policy to reflect changes in law, risk or services and shall communicate material changes where required. The current version shall be available on the platform. Acknowledgement of this Policy does not waive statutory rights.

20 / Company and official contact

HighBinary Technologies Ltd | Company registration number: 17551319 | Registered office: 37th Floor, One Canada Square, Canary Wharf, London, E14 5AA, United Kingdom. Website: https://highbinarytrading.com/ Verification enquiries: support@highbinarytrading.com. Security reports: security@highbinarytrading.com. Submit identity documents only through authorised secure channels; never send passwords, private keys or recovery phrases.