AML & KYC Policy

Our commitment to preventing financial crime.

DOCUMENT	EFFECTIVE	VERSION	ISSUED BY
AML & KYC Policy	**July 2026**	**v2026.1**	**Universal Quantum**

This Anti-Money-Laundering and Know-Your-Customer Policy ("AML Policy") describes the controls Universal Quantum operates to prevent our services being used to launder proceeds of crime, finance terrorism or evade sanctions. It sets out the identity checks that apply to every Account, the monitoring we carry out, the records we keep, and the actions we take when suspicious activity is identified. It is read together with our Terms of Service and Privacy Policy.

1. 1. Purpose

The purpose of this AML Policy is to make sure the Platform is not misused for financial crime, and to explain in plain terms what we ask of investors so we can meet those obligations. The Platform takes a risk-based approach: the checks and documentation we ask for depend on the profile and behaviour of the Account.

2. 2. Regulatory framework

We operate consistent with internationally recognised standards for the prevention of money laundering, terrorist financing and sanctions evasion — including the recommendations of the Financial Action Task Force (FATF), applicable local implementations, and any specific rules that apply in the jurisdictions in which we operate. We update our controls as those standards evolve.

3. 3. Risk-based approach

We assign each Account a risk profile based on factors such as the size of activity, the type and pattern of transactions, geography, source of funds, and negative screening hits. Lower-risk Accounts see standard due-diligence measures; higher-risk Accounts see enhanced measures and, where needed, additional review before further activity is allowed.

4. 4. Know Your Customer (KYC)

Before you deposit, invest or withdraw at material scale, we may require you to verify your identity. Standard KYC collects your full legal name, country of residence, an official government-issued identity document (such as a passport or national ID) and its reference number. You submit this information from your Account through the Verify (KYC) page. We store it securely and use it only for compliance, security and legal purposes.

5. 5. Customer due diligence (CDD)

In addition to the identity data above, we may check public data sources to confirm the information you provided. Where a name or document appears to be inconsistent, we may ask for additional documentation to resolve the discrepancy before allowing further activity.

6. 6. Enhanced due diligence (EDD)

We apply enhanced due diligence to higher-risk situations. That includes, for example, larger transactions, transactions inconsistent with the Account prior activity, connections to higher-risk jurisdictions, or matches against negative-media sources. EDD may involve additional identity documents, evidence of source of funds and source of wealth, and a documented internal review before onboarding or continuing the relationship.

7. 7. Politically exposed persons (PEPs)

Where an Account holder is identified as a PEP, or a close associate of a PEP, we apply enhanced due diligence and senior-level approval before onboarding or continuing the relationship. This does not imply wrongdoing — it reflects the extra scrutiny required by international AML standards for people in positions of public trust.

8. 8. Beneficial ownership

Where the Account is opened for or on behalf of an entity, we may require information about the entity, its ownership structure and the natural persons who ultimately own or control it. We may decline to open or continue an Account if beneficial ownership cannot be clearly identified or evidenced.

9. 9. Ongoing monitoring

KYC is not a one-off event. We monitor Account activity for the life of the relationship. Where the pattern of activity changes materially, where new information comes to light, or where a specific event triggers review, we may re-verify or ask for updated documentation. Failure to respond may result in restrictions on the Account.

10. 10. Source of funds & source of wealth

For higher-risk activity we may ask you to explain and evidence the source of the funds involved in a specific transaction ("source of funds") and, in some cases, how you generally accumulated your assets ("source of wealth"). Common supporting documents include payslips, tax returns, bank statements, or sale contracts. We may pause the transaction until suitable evidence is provided.

11. 11. Transaction monitoring

All deposits and withdrawals are monitored against our fraud and compliance rules. On-chain deposits are matched to the TXID you submit and confirmed on the underlying blockchain. Withdrawals are checked against the wallet address you nominate and against sanctions and negative-media lists. Transactions that hit a rule are held for review before they clear.

12. 12. Sanctions & watchlist screening

We screen Accounts and, where appropriate, counterparties, against applicable sanctions lists and negative-media sources. We do not knowingly provide services to individuals or entities subject to applicable sanctions, or to persons resident in jurisdictions where the service is prohibited by law or by our own risk policies. If a match is confirmed, we will freeze the Account and take the actions required by law.

13. 13. Suspicious activity reporting

If we have grounds to suspect that an Account, transaction or attempt is connected to money laundering, terrorist financing, sanctions evasion, fraud or other financial crime, we file a report with the appropriate authorities in accordance with applicable law and freeze the Account for the period required. We do not "tip off" the person concerned that a report has been filed, as tipping off is itself an offence in most jurisdictions.

14. 14. Record keeping

We keep KYC records, transaction records and internal compliance decisions for the period required by law, which can be several years after Account closure. Records are held securely, access is restricted to authorised staff and audited, and are used only for compliance, security, legal and defence-of-claim purposes, in line with our Privacy Policy.

15. 15. Staff training & culture

Our staff receive regular training on AML rules, sanctions requirements, fraud typologies and how to recognise suspicious activity. A culture of "know your customer" underpins every part of the operation, from onboarding to withdrawals to the way we respond to support tickets.

16. 16. Compliance officer & governance

We designate a person responsible for the day-to-day operation of this AML Policy. That person owns escalation of unusual activity, review of policy exceptions, coordination with authorities, and periodic review of the policy itself. Senior management is briefed on material AML risks and decisions on a regular basis.

17. 17. Prohibited use

Accounts may not be used for money laundering, terrorist financing, sanctions evasion, tax evasion, fraud, market abuse or the funding of illegal activity. Accounts may not be operated on behalf of an undisclosed third party. Any attempt to game rewards or referral programmes through coordinated activity across Accounts is a serious breach and will result in Account closure and forfeiture where lawful.

18. 18. Consequences of non-compliance

Where we identify a breach of this AML Policy, or where we cannot complete the checks we are required to carry out, we may pause activity on an Account, decline a specific transaction, close the Account, withhold funds pending review, report to the relevant authorities, and take any other action required or permitted by law.

19. 19. Cooperation with authorities

We cooperate with law-enforcement agencies, regulators and courts in accordance with applicable law. Where a valid legal request requires us to disclose Account information, freeze funds, or provide records, we do so, log the decision internally, and preserve the records that support it.

20. 20. Reviews & updates

This AML Policy is reviewed on a regular basis and updated when regulatory expectations, our services or our risk profile change. The effective date at the top of the document reflects the latest version. Material updates are announced on the Platform.

21. 21. Detailed provisions & specific measures

Screening technology. We use screening tools to check Account and counterparty details against applicable sanctions lists, politically-exposed-person lists, and negative-media sources. Screening runs both at onboarding and on an ongoing basis. Confirmed matches are escalated to the compliance function for review.

Wire-transfer travel rule. Where a transfer of Digital Assets triggers travel-rule obligations under applicable law, we collect and, where required, transmit the originator and beneficiary information required by the rule to the counterparty institution.

Correspondent-account risk. Where we open, hold or use accounts with other financial or Digital-Asset institutions, we apply due diligence proportionate to the risk of the counterparty, including screening for sanctions exposure, AML programme quality and regulatory standing.

Geographic risk. Our risk model treats certain jurisdictions as higher risk based on published AML and sanctions guidance. Accounts based in, or transacting with, higher-risk jurisdictions may face additional questions, enhanced monitoring, or restrictions on services.

Transaction limits. We may impose per-transaction, daily, or aggregate limits on deposits and withdrawals as a control against money laundering, market abuse and fraud. Limits may be individualised based on your verification level, Account history and risk profile.

Structuring & smurfing. Splitting a single logical transaction into several smaller pieces to avoid limits or reporting thresholds is a serious breach. Where structuring is suspected, we treat the pattern as a single transaction, apply the appropriate controls, and where indicated, file a suspicious-activity report.

Exit management. Where we close an Account for AML reasons, we return the net Available Balance to a wallet address consistent with the verified identity on the Account, subject to any restriction imposed by law. In some cases funds may need to be held pending review or authorisation from an authority.

Third-party payments. We do not accept deposits from, or make withdrawals to, wallets known to belong to a third party. Every deposit is treated as coming from, and every withdrawal as going to, the Account holder. Attempts to use a third party as an intermediary are treated as a breach of this Policy.

Adverse-media checks. Adverse-media hits (for example press coverage linking a person to fraud or organised crime) trigger enhanced due diligence and, where confirmed, may result in restrictions on the Account. Where a hit is a case of mistaken identity, we welcome supporting evidence that helps us close the alert.

Independent review. Our AML controls and their operation are subject to periodic review to make sure they remain adequate and are being followed. Findings from those reviews feed into policy and technology updates.

Regulatory reporting. We file the reports required by applicable law with the appropriate authorities, on the timelines the law prescribes. We keep records of every filing.

Cooperation on court orders. Where a valid court order or an equivalent lawful instrument requires us to freeze funds, produce records or take any other action, we comply with the order and record the decision. Where we are permitted to notify you, we do.

Whistleblowing. Staff and third parties who have concerns about AML compliance on the Platform can raise those concerns through the contact channel. Reports are treated confidentially and are handled by the compliance function.

Investor duties. Investors are expected to answer verification questions honestly and promptly, to keep their contact and identity details current, and to alert us promptly if they suspect their Account has been misused. Failure to do so may result in restrictions on the Account.

22. 22. Glossary

AML — Anti-Money-Laundering: the framework of laws, controls and processes designed to prevent financial systems being used to launder proceeds of crime.

CDD — Customer Due Diligence: the standard identity checks applied to an Account.

EDD — Enhanced Due Diligence: additional checks applied to higher-risk Accounts or transactions.

FATF — The Financial Action Task Force: an intergovernmental body that sets global AML and counter-terrorist-financing standards.

KYC — Know Your Customer: the process of verifying an Account holder identity and confirming the details provided at onboarding.

PEP — Politically Exposed Person: an individual who holds, or has recently held, a prominent public function, along with certain close family members and associates.

SAR — Suspicious Activity Report: a report filed with the appropriate authority when there are grounds to suspect financial crime.

Structuring — Splitting a transaction into smaller pieces with the aim of avoiding limits or reporting thresholds.

Travel rule — The requirement to transmit originator and beneficiary information alongside certain qualifying transfers.

Tipping off — Disclosing to a person that a suspicious-activity report has been filed against them, which is itself an offence in many jurisdictions.

Sanctions — Restrictions imposed by governments or international bodies on named persons, entities or jurisdictions.

Beneficial owner — The natural person or persons who ultimately own or control an Account or a transaction.

Source of funds — The origin of the specific funds used in a transaction.

Source of wealth — How you generally accumulated your overall wealth, distinct from the funds used in a single transaction.

23. 23. Contact

Compliance questions and evidence submissions can be raised through the contact page. Please mark the subject line "Compliance" so the right team receives it promptly.