AML, Sanctions and Financial Crime Policy

The division of responsibility with Binance, and the controls Tenxex operates in its own right.

Document	TENXEX-LEG-004 – AML, Sanctions and Financial Crime Policy
Version / Status	Version 1.4 – Approved for publication
Effective date	14 August 2026
Issued by	Tenxex Exchange Corp. (“Tenxex”, “we”, “us”, “our”), registered in the British Virgin Islands, registered office at 2nd Floor, Ritter House, Wickham's Cay II, Tortola, British Virgin Islands
Operating model	Tenxex Exchange Corp. operates a customer-facing trading interface integrated with Binance’s API. Binance provides the underlying trading infrastructure, liquidity, execution, KYC/AML and, where applicable, custody. Tenxex Exchange Corp. receives an agreed commission based on transaction activity generated through the platform
Partner programme	Binance Partner Programme, governed by the partner agreement between Tenxex Exchange Corp. and Binance
Authorisations	Tenxex Exchange Corp. is registered in the British Virgin Islands. Any applicable regulatory licences or registrations should be stated here only where actually obtained
Website	tenxex.com
Document owner	Compliance Officer and MLRO, Tenxex Exchange Corp.
Review cycle	At least annually, and on material change to law, business model or the Binance arrangement

Customer identity verification (KYC), customer due diligence, transaction monitoring, travel-rule compliance and suspicious activity reporting in respect of user accounts and transactions are performed by Binance as the regulated venue. This Policy describes the financial crime controls that Tenxex Exchange Corp. operates in its own right as an interface provider, and how it cooperates with Binance and with competent authorities.

1. Purpose and Scope

1.1 Tenxex Exchange Corp. is committed to ensuring that its Platform is not used to facilitate money laundering, terrorist financing, proliferation financing, sanctions evasion, fraud or any other financial crime.

1.2 This Policy applies to all employees, officers, contractors and agents of Tenxex, to all Platform users, and to all commercial counterparties, introducers, affiliates and suppliers.

1.3 It is a client-facing summary. The full internal policy, risk assessment, control matrix and procedures are confidential and are provided to competent authorities, auditors, banking partners and Binance on request.

2. Division of Responsibility

2.1 Tenxex operates a customer-facing trading interface integrated with Binance's API. Binance provides the underlying trading infrastructure, liquidity, execution, KYC/AML and, where applicable, custody. The allocation of financial crime responsibilities follows that structure.

Control	Performed by Binance	Performed by Tenxex
Customer identification and verification (KYC)	Yes – identity, documents, biometric liveness, address and account-level verification	No – Tenxex does not collect or hold identity documents or verification data
Customer due diligence, EDD, PEP and adverse media screening	Yes – at account level, on an ongoing basis	No, save for the counterparty due diligence in section 5
Source of funds and source of wealth enquiry	Yes	No
Custody of, and controls over, client fiat and crypto-assets	Yes, where applicable	No – Tenxex never holds or controls user assets
Transaction monitoring and blockchain analytics	Yes – across accounts and on-chain activity	Limited – behavioural and abuse monitoring of Platform usage only
Travel Rule information transmission	Yes	No
Suspicious transaction reporting to a financial intelligence unit	Yes, in respect of account and transaction activity	Yes, in respect of its own knowledge or suspicion, where a reporting obligation applies to Tenxex
Sanctions and restricted-jurisdiction screening of Platform access	At account level	Yes – at interface access level, as described in section 4
Marketing and promotional compliance	Own channels	Yes – for all Tenxex channels

2.2 Reliance on Binance for account-level controls does not reduce Tenxex's own accountability for the controls it operates, nor its duty to report knowledge or suspicion of financial crime where a legal obligation applies to it.

2.3 Where a banking partner, correspondent institution, regulator or Binance imposes a higher standard than this Policy, the higher standard applies.

3. Governance

3.1 The Board approves this Policy, sets the financial crime risk appetite, and receives reporting on the effectiveness of the framework at least annually. A named member of senior management is accountable for financial crime compliance.

3.2 A Compliance Officer and Money Laundering Reporting Officer (**MLRO**) is appointed with sufficient seniority, independence and resources, and with unrestricted access to records and systems. The MLRO assesses internal reports and makes external reports where required.

3.3 A documented business-wide financial crime risk assessment is maintained and reviewed at least annually and on material change to the business model, the Binance arrangement, the user base, the jurisdictions served or the threat environment.

3.4 No employee suffers detriment for reporting a suspicion in good faith. Confidential internal reporting and whistleblowing channels are maintained.

4. Sanctions and Geographic Access Controls

4.1 Tenxex maintains a Restricted Jurisdictions list, published on the Platform, covering jurisdictions subject to comprehensive sanctions, jurisdictions where Tenxex is not permitted to offer the Platform, and jurisdictions excluded on a risk basis.

4.2 Access controls include registration-time declarations, IP-based geolocation blocking, detection of VPN, proxy and anonymising infrastructure, device and behavioural signals, and blocking of access from restricted locations.

4.3 Platform users, and all commercial counterparties, are screened against consolidated sanctions lists administered by the United Nations, European Union, the United States Office of Foreign Assets Control, the United Kingdom and other applicable authorities, at onboarding and on an ongoing automated basis against list updates.

4.4 A positive or potential match results in immediate suspension of Platform access pending review, escalation to the MLRO, notification of Binance where the account relationship is affected, and reporting to the competent authority where required.

4.5 Deliberate circumvention of geographic or sanctions controls is a material breach of the Terms of Use, results in permanent loss of access, and is reported.

5. Counterparty, Partner and Supplier Due Diligence

5.1 Due diligence is performed before onboarding any introducer, affiliate, marketing partner, payment provider or material supplier, covering ownership and control, beneficial owners, sanctions and adverse media screening, licensing status where relevant, and the integrity of the commercial arrangement.

5.2 Introducer and affiliate arrangements are documented in writing, prohibit misleading or non-compliant promotion, prohibit the offering of unauthorised rebates or inducements, and are subject to periodic review and audit.

5.3 Payments of commission or referral fees are made only to verified counterparties, in their own name, through traceable banking or on-chain rails, and never in cash.

6. Prohibited Use and Users

6.1 The Platform must not be used by, or for the benefit of:

- any person subject to applicable sanctions, or owned or controlled by such a person;
- any person located in or accessing from a Restricted Jurisdiction;
- any person under 18 years of age or lacking legal capacity;
- any person trading on behalf of an undisclosed third party, or using another person's Binance account or API Key;
- operators of darknet marketplaces, ransomware, malware distribution, human trafficking, arms or narcotics trafficking, or terrorist financing;
- Ponzi and pyramid schemes, fraudulent investment schemes and unlicensed gambling operators;
- unlicensed money service businesses, unlicensed brokers and nested-access arrangements offering onward trading services to their own customers through a Tenxex profile.

6.2 The Platform must not be used to engage in market abuse, including wash trading, spoofing, layering, ramping, insider dealing or coordinated manipulation. Such conduct is reported to Binance and, where required, to competent authorities.

6.3 Tenxex does not accept payments from users in connection with trading and does not hold user assets. Any attempt to route funds through Tenxex is refused and investigated.

7. Platform-Level Monitoring

7.1 Tenxex monitors Platform usage for indicators of abuse and financial crime, including: registration and login anomalies; device, IP and geolocation inconsistencies; use of anonymising infrastructure; clustering of profiles sharing devices, addresses or contact details; patterns consistent with account takeover, coercion or third-party control; automated or scripted abuse; and behaviour consistent with scam typologies affecting the user.

7.2 Alerts are triaged, investigated and documented within defined service levels. Outcomes may include requests for information, restriction or termination of Platform access, notification to Binance, and internal escalation to the MLRO.

7.3 Monitoring at Platform level supplements, and does not replace, Binance's account-level transaction monitoring.

8. Reporting, Cooperation and Tipping Off

8.1 All employees must report internally, promptly and without conducting their own external enquiries, any knowledge or suspicion of money laundering, terrorist financing, sanctions breach, fraud or other financial crime.

8.2 The MLRO assesses each internal report and, where a reporting obligation applies to Tenxex, submits a report to the competent financial intelligence unit in the applicable jurisdiction within the required timeframe.

8.3 Tenxex cooperates fully with lawful requests from competent authorities, and with requests from Binance made in connection with its regulatory obligations, subject to applicable data protection law and to any legal restriction on disclosure.

8.4 Employees must not disclose to a user or any third party that a report has been made or is contemplated, or that an investigation is under way. Unauthorised disclosure may be a criminal offence.

9. Record Keeping

9.1 Screening results, access restriction decisions, internal reports, MLRO assessments, external reports, counterparty due diligence and related correspondence are retained for at least five (5) years from the date of the record or the end of the relationship, and for longer where required by law or by a competent authority.

9.2 Records are held securely, are retrievable without undue delay, and are processed in accordance with the Privacy Policy.

10. Training

10.1 All staff receive financial crime and sanctions training at induction and at least annually, with enhanced role-specific training for support, operations, marketing and compliance staff, and briefings for the Board.

10.2 Training covers applicable obligations, the division of responsibility with Binance, crypto-asset typologies, red flags, internal reporting duties, tipping-off prohibitions and personal liability. Attendance and comprehension are recorded and tested.

11. Assurance and Review

11.1 The framework is subject to independent review by internal audit or an external specialist at least annually, covering control design, operating effectiveness, screening calibration, alert quality, record keeping and training.

11.2 Findings are reported to the Board with tracked remediation, owners and target dates. The MLRO produces an annual report on the operation and effectiveness of the framework.

11.3 This Policy is reviewed at least annually, and on any material change to law, the business model or the arrangement with Binance.

12. User Obligations and Contact

12.1 Users must provide accurate information, must comply with all information requests from Binance, and must not attempt to circumvent any control described in this Policy.

12.2 Questions, due diligence questionnaires and requests for the compliance pack should be sent to compliance@tenxex.com, marked for the attention of the MLRO. Suspected fraud or account compromise should be reported immediately to security@tenxex.com and to Binance.

End of AML, Sanctions and Financial Crime Policy.