Anti-Money Laundering (AML) & Counter-Terrorist Financing (CTF) Policy

For: Neuralogic Sp.z.o.o - Crypto Asset Exchange / Virtual Asset Service Provider (VASP) in MiCA Jurisdiction

---

1. Purpose and Scope

This AML & CTF Policy (“Policy”) sets out the principles, controls, and procedures adopted by the Exchange to prevent, detect, and report money laundering (“ML”), terrorist financing (“TF”), proliferation financing (“PF”), and other financial crimes, in line with applicable laws, regulations, and international standards, including FATF Recommendations and the EU Markets in Crypto-Assets Regulation (MiCA) requirements.

This Policy applies to: - The Exchange, its branches, subsidiaries, and affiliates (where applicable) - All directors, officers, employees, contractors, and agents - All products, services, customers, and jurisdictions in which the Exchange operates

---

2. Regulatory Framework and Standards

The Exchange commits to compliance with all applicable AML/CTF laws and regulations, including but not limited to: - FATF Recommendations and Interpretive Notes - EU Anti-Money Laundering Directive (AMLD5/6) and national AML legislation - Markets in Crypto-Assets Regulation (MiCA) requirements, including obligations for crypto-asset service providers (CASPs) - Applicable local AML/CTF legislation in the Exchange’s licensing jurisdiction(s) - Sanctions regimes issued by the UN, EU, OFAC, HMT, and other competent authorities - Travel Rule requirements for virtual asset transfers - Data protection and privacy laws (e.g., GDPR, where applicable)

Where multiple standards apply, the higher standard shall prevail.

---

3. Governance and AML Framework

3.1 Board and Senior Management Oversight

The Board of Directors bears ultimate responsibility for AML/CTF compliance and shall: - Approve this Policy and any material amendments - Ensure adequate resources, systems, and controls - Oversee AML/CTF risk management -

Receive periodic AML/CTF reports, including MiCA-specific reporting requirements

3.2 Compliance Function

The Exchange maintains an independent Compliance Function responsible for: - Developing and maintaining AML/CTF policies and procedures in line with MiCA and other applicable standards - Monitoring regulatory developments, including MiCA implementation updates - Advising business units on AML/CTF and MiCA compliance matters

3.3 Money Laundering Reporting Officer (MLRO)

The MLRO (and Deputy MLRO, if applicable) shall: - Act as the primary point of contact with regulators and Financial Intelligence Units (FIUs) - Receive and assess internal suspicious activity reports - File Suspicious Transaction/Activity Reports (STR/SAR) in line with MiCA requirements - Oversee transaction monitoring and investigations - Maintain AML records and reporting consistent with MiCA and local obligations

---

4. Risk-Based Approach (RBA)

The Exchange adopts a risk-based approach to AML/CTF, identifying and mitigating risks associated with: - Customers - Products and services - Delivery channels - Geographic exposure

Risk assessments are: - Documented - Reviewed at least annually - Updated upon material changes to the business, regulatory environment, or MiCA guidance

---

5. Customer Due Diligence (CDD)

5.1 Customer Identification and Verification

The Exchange shall identify and verify customers prior to establishing a business relationship, including: - Full legal name - Date of birth / incorporation - Nationality / jurisdiction of incorporation - Residential / registered address - Government-issued identification or corporate documents

Verification shall be conducted using reliable, independent sources.

5.2 Customer Types

CDD requirements apply to: - Individual customers - Corporate customers - Trusts, foundations, and other legal arrangements

5.3 Beneficial Ownership

For legal entities, the Exchange shall: - Identify beneficial owners holding 25% or more (or lower thresholds where required by MiCA or national laws) - Verify beneficial owners' identities - Understand ownership and control structures

---

6. Enhanced Due Diligence (EDD)

EDD shall be applied to higher-risk customers, including but not limited to: - Politically Exposed Persons (PEPs) - Customers from high-risk or sanctioned jurisdictions - High-volume or complex trading profiles - Privacy-enhancing technologies and mixers (where permitted)

EDD measures may include: - Source of funds and source of wealth verification - Senior management approval - Increased transaction monitoring

---

7. Sanctions Screening

The Exchange conducts real-time and periodic screening against: - International sanctions lists - Watchlists and adverse media databases

Any positive or potential matches shall be escalated to Compliance immediately and, where required, assets shall be frozen and authorities notified, consistent with MiCA provisions.

---

8. Transaction Monitoring

8.1 Ongoing Monitoring

The Exchange employs automated and manual monitoring systems to detect unusual or suspicious activity, including: - Structuring or layering patterns - Rapid in-and-out movements - High-risk wallet interactions - Unusual trading behavior

8.2 Blockchain Analytics

The Exchange uses blockchain analytics tools to: - Identify high-risk wallets - Trace transaction flows - Detect links to illicit activities

---

9. Suspicious Activity Reporting

9.1 Internal Reporting

Employees must report any suspicious activity promptly to the MLRO.

9.2 External Reporting

Where suspicion is confirmed, the MLRO shall file STRs/SARs with the relevant FIU within statutory timelines, including MiCA-mandated reporting obligations.

Tipping-off is strictly prohibited.

---

10. Travel Rule Compliance

The Exchange complies with applicable Travel Rule requirements by: - Collecting and transmitting required originator and beneficiary information - Implementing secure data-sharing mechanisms - Ensuring counterparty VASP due diligence - Maintaining records for audit purposes in line with MiCA

---

11. Record Keeping

The Exchange retains AML/CTF records for a minimum of five (5) years or longer if required by law or MiCA, including: - CDD and EDD records - Transaction data - STR/SAR filings - Risk assessments and audit reports

---

12. Employee Screening and Training

12.1 Employee Screening

All employees are subject to: - Background checks - Fit and proper assessments for sensitive roles

12.2 Training

Mandatory AML/CTF and MiCA-compliance training is provided: - Upon onboarding - Annually thereafter - When material regulatory changes occur

---

13. Independent Audit and Testing

The AML/CTF framework shall be subject to: - Periodic independent audits - Internal control testing - Remediation tracking - MiCA-specific compliance assessments

---

14. Data Protection and Confidentiality

All AML/CTF activities shall be conducted in compliance with applicable data protection laws, ensuring confidentiality and secure handling of personal data.

---

15. Breaches and Disciplinary Measures

Breaches of this Policy may result in: - Disciplinary action - Termination of employment or contracts - Regulatory reporting where required

---

16. Policy Review and Updates

This Policy is reviewed at least annually and updated to reflect: - Regulatory changes, including MiCA - Business developments - Identified weaknesses or incidents

---

Approved by: Board of Directors
Effective Date: January 2026
Last Review Date: January 2026