ANTI-MONEY LAUNDERING (AML) POLICY

Nuvvex Global S.R.O

1. Introduction

Nuvvex Global S.R.O is a virtual currency exchange and virtual currency wallet company, acting according to the laws of the Czech Republic. The Company is committed to conduct business operations in a transparent and open manner consistent with its regulatory obligations.

This Anti-Money Laundering (AML) Policy aims to establish robust measures to prevent, detect, and report money laundering and terrorist financing activities associated with our cryptocurrency exchange operations in the Czech Republic. This policy demonstrates our commitment to compliance with applicable laws and the integrity of our operations.

2. Scope

This policy applies to all employees, directors, and affiliates of Nuvvex including external contractors, service providers (consultants). It covers all activities related to the exchange of cryptocurrencies and digital assets, including trading, deposit, and withdrawal processes.

3. Legal Framework

We adhere to relevant Czech laws and regulations, including but not limited to:

- Act No. 253/2008 Coll., on Selected Measures Against Legitimization of Proceeds of Crime and Financing of Terrorism (AML Act)
- European Union Anti-Money Laundering Directives (AML D)
- Czech National Bank (CNB) regulations and guidelines

4. Risk Assessment

We will conduct comprehensive risk assessments to identify and evaluate the risk of money laundering and terrorist financing inherent in our operations, taking into account:

- Customer profiles and behaviors
- Types of cryptocurrencies offered
- Geographical risks
- Transaction patterns and volumes
- Product, Service, Transaction or Delivery channel risk factors

Risk Level Assessment Matrix

Low	Moderate	High
Stable, known client / return	Client who did up a few transactions	New Client
The client is located in high tax rate jurisdiction	There is a moderate tax rate in the client's jurisdiction	There is very low tax rate in the client's jurisdiction
Whether the origin of the client’s assets or the source and origin of the funds used for a transaction can be easily identified		Whether the origin of the client’s assets or the source and origin of the funds used for a transaction can't be identified

very low amount of transaction up to 1K	Moderate amount of transaction 1-5K	amount of transaction above 5K
Whether the jurisdictions isn't involved apply legal provisions that are in compliance with the international standards of AML/CTF	The client is located in an area known to have moderate crime rate and included in international sanction lists	The client is located in an area known to have high crime rate and included in international sanction lists
The client is located in an area known to have low crime rate and included in international sanction lists	The client is located in an area known to have moderate crime rate and included in international sanction lists	The client is located in an area known to have high crime rate and included in international sanction lists
Age of the client 22-45	Age of the client 45-70	Age of the client 70-80

5. Customer Due Diligence (CDD)

- 5.1 Identification and Verification
  We will implement CDD measures, including:
    - Verifying customer identities using government-issued identification documents prior to making a business relationship
    - Collecting information about the customer's source of funds

- 5.2 Simplified Due Diligence (SDD)
  Simplified due diligence (SDD) is the minimum level of due diligence that must be applied to the customer. SDD may be carried out when the Company assesses customer's risk as Low and one of the following conditions are fulfilled,
    - Customer is a listed company (EU or equivalent)
    - Customer is a government or municipality institution

  SDD is not permitted if there are mandatory conditions to perform EDD or CDD.

  When applying SDD, Company must:
    - For individuals – obtain name, surname and personal number
    - For business customers – obtain name, legal form, registered office/address, address of actual operation, registration number (if such number has been issued).
    - Get customer's first top-up from his/her bank, payment or electronic money account in EU or third country having same level as Lithuanian AML requirements.
    - Ensure ongoing monitoring of the business relationship
    - Regularly check if the customer is still eligible for SDD

- 5.3 Enhanced Due Diligence (EDD)

  For high-risk customers, including politically exposed persons (PEPs), enhanced measures will include:
    - Additional verification of identity
    - Detailed understanding of the nature of the customer's business

- More frequent monitoring of transactions including countries identified by the Financial Action Task Force (FATF) as High Risk.

6. Reporting Suspicious Activities

- 6.1 Identification
  Employees are trained to recognize signs of suspicious transactions, including unusual deposit or withdrawal patterns.

6.2 Reporting

Suspicious activities must be reported immediately to the designated AML Compliance Officer.

6.3 Filing Suspicious Activity Reports (SARs)

The AML Compliance Officer is responsible for evaluating the need to file a SAR with the Financial Analytical Office (FAÚ) or other relevant authorities.

7. Record Keeping

We will maintain comprehensive records of all transactions, customer identification documents, and reports of suspicious activities for up to 10 years, in accordance with the AML Act.

8. Employee Training

All employees will undergo AML training that includes:

- Overview of AML laws and regulations
- Identification of suspicious activities and red flags
- Internal reporting procedures and protocols
- Training will be conducted upon hiring and updated regularly for all employees and other individuals who act on behalf of the Company to make sure that those who have contact with customers, who see customer transaction activity understands the reporting, customer identification and record keeping requirements.

9. Compliance Monitoring and Audit

Regular internal audits will be conducted to assess compliance with AML policies and procedures. Any identified non-compliance will be addressed with corrective actions.

10. Policy Review and Updates

This AML policy will be reviewed annually and updated as necessary to align with regulatory changes and industry best practices. Employees will be informed of significant updates.

11. Consequences of Non-Compliance

Failure to adhere to this AML policy may result in disciplinary actions, including termination of employment, and potential legal repercussions.

12. Commitment to Integrity

Nuvvex is dedicated to fostering a culture of compliance, integrity, and transparency. We will take all necessary steps to prevent money laundering and terrorist financing, ensuring the security and trust of our customers and the broader financial system.

Conclusion

This AML Policy outlines our commitment to preventing financial crimes within our cryptocurrency exchange operations. All employees are expected to understand and adhere to these guidelines to protect our organization and comply with Czech regulations.

Appendix A

SUSPICIOUS TRANSACTION REPORT
For Money Laundering and Funding of Terrorism

Date:		Report Ref. No.	

Check appropriate box:	Initial Report: ☐	Supplemental Report: ☐	

Previous Connected Reports:	Ref. No. _____	Ref. No. _____

Part 1. Subject of Report

Full of Suspect (including aliases and/or nickname(s)			
Identification: Type and document number (If available, copy to be attached to this report):			
Identity Card: ☐	Passport: ☐	Other – Specify: ☐	
No:	No:	No:	
Expires:	Expires:	Expires:	

Address:			
Date of Birth / Registration:			
Occupation / Nature of Business:			
Nationality / Country of Incorporation:			
Date Business Relationship was established:			
Type of Products (Accounts, Policies, Usernames, etc.) held with institution, if any:	(one product per box)	(one product per box)	(one product per box)
Product/Relationship (Accounts, Policies, Usernames, etc.) Number			

Date of Opening/Closing of Product (Account, Policy, etc)			
Balance at Report Date:			

Name of the MLRO (in Block letter)	Signature of MLRO _____

Part 2. Suspicious Transaction / Activity

Date:	Amount	Source

Explanation/description of suspicious transaction /activity The STR should be described in a complete and clear manner. All facts should be given in a chronological order including what is unusual, irregular or suspicious about the transaction/activity being reported. All relevant information used by the MLRO supporting documentation that is likely to assist the FMA in its analysis should be attached to this report. **(Annex additional sheets if required.)**
List of Documents attached:

Name of the MLRO (in Block letter)	Signature of MLRO _____

Appendix B

Nuvvex – declaration of buying crypto currency

Declaration of Deposit

I hereby confirm that the below transactions were done solely by me via Uppex.com website for the purpose of buying crypto currency.

I certify that I am the authorized bank account or credit/debit cardholder. In case of a joint account, I authorize the account holder to use my card or bank account. By submitting these payments to the system, I am aware that the rate of the exchange, and all subsequent fees for the transaction, will be determined by Nuvvex at the time of execution and no refunds or cancellation of the transaction will be permitted after it has been approved. I also agree to all Terms and Conditions of Nuvvex. I also declare I made the purchase by myself, and not for third party.

Bank Wire Transfer:

Date of Deposit (dd/mm/yyyy)	Amount and Currency	Signature

Bank Name:	
Bank Address:	
SWIFT / BIC:	
IBAN:	
Account Name:	
Account Holder Address:	
Account Number:	
Additional Information:	

Clients Crypto E-Wallet Address:	