DIGITAL META BANK

LEGAL POLICY

ANTI-MONEY LAUNDERING, COUNTER-TERRORISM FINANCING AND WEAPONS OF MASS DESTRUCTION PROLIFERATION PREVENTION POLICIES (AML/CTF)

NEO BANKERS
INNOVATION OF THE QUINTESSENCE

RE: **DISCLAIMER:**
We hope you find this content useful.
This content is for general information only, not legal or financial advice. NEO BANKERS LLC disclaims all liability for actions based hereon. It's not legal advice. Seek professional counsel before acting.

Abstract

Anti-Money Laundering, Counter-Terrorism Financing and Weapons of Mass Destruction Proliferation Prevention Policy

This Anti-Money Laundering, Counter-Terrorism Financing and Weapons of Mass Destruction Proliferation Prevention Policy (AML/CTF) including the Know Your Customer (KYC) User Identification and Verification Policy (collectively referred to as the Anti-Money Laundering Policy) has been set by LLC "NEO BANKERS", a company registered and operating in accordance with the legislation of Poland, KRS (National Court Register) code 0000981293, registered at the address: Złota 61/101, 00-819 Warsaw, Poland (hereinafter referred to as Neo Bankers, the Service) to apply when registering Users at https://neobankers.io as well as during further interaction with the User when fulfilling the User's Applications in accordance with the User Agreement and other documents posted at https://neobankers.io/faq/terms/ and binding on the User.

This Policy is developed in compliance with:

a) The Act of 1 March 2018 on Counteracting Money Laundering and Terrorist Financing, as amended (Polish Journal of Laws of 2022, item 593, 655, 835, 2180, 2185);
b) Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, as amended by Directive (EU) 2018/843 (5th AML Directive);
c) Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019 laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences;
d) Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on Markets in Crypto-assets (MiCA);
e) International standards set by the Financial Action Task Force (FATF).

In accordance with international and local regulations, NEO BANKERS implements effective internal procedures and mechanisms to prevent money laundering, terrorist financing, drug and human trafficking, proliferation of weapons of mass destruction, corruption and bribery, and response to any form of suspicious activity on the part of its Users. This Policy includes the verification procedure and the presence of an appointed officer responsible for the compliance with AML, Transaction Monitoring and Risk Assessment standards.

DIGITAL META BANK

LEGAL POLICY

ANTI-MONEY LAUNDERING, COUNTER-TERRORISM FINANCING AND WEAPONS OF MASS DESTRUCTION PROLIFERATION PREVENTION POLICIES (AML/CTF)

NEO BANKERS
INNOVATION OF THE QUINTESSENCE

RE: **DISCLAIMER:**

We hope you find this content useful.

This content is for general information only, not legal or financial advice. NEO BANKERS LLC disclaims all liability for actions based hereon. It's not legal advice. Seek professional counsel before acting.

By registering at https://neobankers.io, the User (a legal entity or an individual) thereby confirms that they have read the Anti-Money Laundering Policy, accept their terms and conditions and undertake to provide the Service with all the necessary data and documents required for identification and verification of the User and stipulated by the Policy. Anti-Money Laundering Policy is periodically reviewed and amended based on prevailing industry standards and international regulations to help prevent illegal activities, including money laundering and terrorist financing. All NEO BANKERS key management personnel, employees and customers are required to acknowledge and familiarize themselves with the Policy.

The Policy is implemented to:

A. Prevent the intentional or unintentional use of NEO BANKERS for money laundering or terrorist financing, in accordance with Article 1 of Directive (EU) 2015/849.
B. Give NEO BANKERS the opportunity to better know/understand its Users, platform users, business partners and other contacts with whom NEO BANKERS cooperates in any manner (hereinafter referred to as the Users), as required by Article 13 of Directive (EU) 2015/849.
C. Establish appropriate control measures to identify and report suspicious activity in accordance with the applicable laws, procedures and regulations, as mandated by Article 33 of Directive (EU) 2015/849.
D. Provide Neo Bankers employees with the necessary materials to resolve issues related to KYC/AML procedures and reporting obligations, in line with Article 46 of Directive (EU) 2015/849.

RE: **DISCLAIMER:**
We hope you find this content useful.
This content is for general information only, not legal or financial advice. NEO BANKERS LLC disclaims all liability for actions based hereon. It's not legal advice. Seek professional counsel before acting.

RISK ASSESSMENT POLICY

NEO BANKERS adopts and maintains the Risk-Based Approach (RBA) to assess and limit the money laundering and terrorist financing risks for NEO BANKERS arising from any transactions performed by its Users, in accordance with Article 8 of Directive (EU) 2015/849. The guiding principles are as follows:

A. Before making any transaction or proposed transaction, it is vital to carry out the necessary checks in accordance with the RBA to ensure that the identity of the User does not match any wanted person or person on the sanctions lists; that the User is not a terrorist and is not a member of any terrorist organizations. Such checks are carried out at https://mf-arch2.mf.gov.pl/en/web/bip/ministry-of-finance/aml-ctf/sanctions or on any other resource containing a confirmed up-to-date list of persons associated with terrorist activities or being subject to international sanctions; it also checked that the User's identity does not match any of the lists of persons (legal entities and individuals) being subject to personal or special economic and other restrictive measures (sanctions) in accordance with the current resources of the Ministry of Finance of Poland (https://www.gov.pl/web/finance/sanctions-aml-ctf).
B. In order to classify the risk, the relevant information must be obtained from the User before making a transaction or establishing any business relations, as required by Article 13 of Directive (EU) 2015/849.
C. Risk classification for different types of Users may take into account the nature of their business, the location of the User, country of origin, sources of funds, payment methods, turnover volume, and social and financial background, in line with Annex III of Directive (EU) 2015/849.
D. Risk classification results should be obtained based on the relevant information provided by the User when establishing any business relations.
E. High-risk Users will require an enhanced due diligence review, especially the Users with unclear sources of funds or high-frequency transactions, which are determined by NEO BANKERS in its sole and absolute discretion, in compliance with Article 18 of Directive (EU) 2015/849.
F. Neo Bankers must be able to convince the competent authorities that the due diligence review has been carried out based on the Users' risk profile in accordance with the applicable law.
G. Should NEO BANKERS deem it necessary, NEO BANKERS may appoint a third-party KYC/AML specialized firm to ensure compliance with the applicable NEO BANKERS rules and policies. NEO BANKERS must ensure that such third party is properly regulated, monitored and complies with all the requirements necessary to verify the Users and maintain documentation in accordance with the applicable regulations, and that such third party is not based in any high-risk country or jurisdiction.

ANTI-MONEY LAUNDERING, COUNTER-TERRORISM FINANCING AND WEAPONS OF MASS DESTRUCTION PROLIFERATION PREVENTION POLICIES (AML/CTF)

RE: **DISCLAIMER:**

We hope you find this content useful.

This content is for general information only, not legal or financial advice. NEO BANKERS LLC disclaims all liability for actions based hereon. It's not legal advice. Seek professional counsel before acting.

I. ASSIGNING A VERIFIED NEO BANKERS STATUS / WHITELISTING:

A. Establishing and maintaining risk-based customer due diligence review, identifying, verifying and carrying out KYC procedures based on risk assessment including enhanced due diligence review for high-risk Users such as politically exposed persons (PEPs) and public figures. Checking whether the Users are politically exposed persons or public figures can be carried out at https://mf-arch2.mf.gov.pl/en/web/bip/ministry-of-finance/aml-ctf/sanctions

B. NEO BANKERS must not permit the activation or maintenance of any whitelisted anonymous accounts in a fictitious name or accounts on behalf of others whose identity has not been disclosed or cannot be verified.

C. In order to be assigned a verified status, the User must fulfil all the requirements of this Policy by providing information and copies of documents stipulated by this Policy. The Service reserves the right to periodically update the User's information and conduct additional checks to confirm the verified status. Based on the results of such checks, the Service may refuse to confirm the verified status to the User without giving a reason.

II. INTERNAL CONTROL

The Service applies the rules of internal control in order to ensure that the transactions performed using the Service comply with the requirements of the legislation on anti-money legalization (laundering), counter-terrorism financing and weapons of mass destruction proliferation prevention, in particular, with the requirements of the current Act of 1 March 2018 on counteracting money laundering and terrorist financing (https://mf-arch2.mf.gov.pl/documents/764034/1010418/ustawa+tekst_EN+_15062018-f+_16072018.pdf). Some of these internal control measures are listed in this document and may include, but are not limited to the User Identification Program, the Suspicious Activity Reporting System and the required reports on the effectiveness of the Policies for Neo Bankers key management personnel.

III. USER IDENTIFICATION AND VERIFICATION PROGRAM GENERAL PROVISIONS

A. The User identification program should be implemented at the following stages:

(i) when establishing a business relationship
(ii) before or during any financial transaction; and
(iii) when there is any doubt about the authenticity/reliability or adequacy of the previously obtained identification data of the User

B. NEO BANKERS:

(i) will require the User to provide a certificate of identity; and
(ii) will under no circumstances allow to process any transaction above 0.5 BTC or the equivalent of another cryptocurrency or fiat currency when having incomplete information about the User or without requiring additional information to verify their identity, in compliance with Article 115 of Regulation (EU) 2023/1114 (MiCA).

C. In case there is any suspicion of money laundering or terrorist financing activities, or when there are any doubts about the adequacy or reliability of the previously obtained identification data of the User, the Service will take measures and carry out a due diligence review including re-checking the identity of the User and obtaining information about the purpose and the intended nature of their business relations with NEO BANKERS.

D. Electronic Payment Systems, which may be reporting institutions in accordance with the legislation of their countries of registration, may use the identification data the User has provided to the Service to perform financial transactions and identify the User as a sender/recipient of a money transfer. If necessary, the Electronic Payment Systems may request additional information from the User including documentary confirmation of the source of the User's funds. If the User fails to provide the requested information and documents, the Electronic Payment System has the right to deny transactions and request the Service to assign an increased risk category to such User.

IV. PROCEDURE FOR IDENTIFYING AND VERIFYING USERS

A. The following identification data must be obtained for verifying individuals:
- Full name
- Date and place of birth
- Citizenship
- State identification number (where applicable), i.e., national ID card number or passport number
- Sex
- Registration address (for citizens of the European Union)
- Actual residence address. Such address is confirmed by receiving a copy of the document confirming the address (one or more, at the discretion of Neo Bankers) issued at least 3 months before the activation of an account. The document must contain the name and address of the User.
- Correspondence address (if different from the registration address and actual residence address). Identification and verification of proxy holders (if the User has provided a power of attorney to use their account (proxy holder registration) is carried out in the same way as identification and verification of the account owner

B. The following information and documentation must be obtained for verifying legal entities:
- Full legal name
- Identification code
- Government-issued identity documents (for related parties)
- Address confirmation for related parties (issued within 3 months of receipt)
- Registration certificate
- COI
- M&AA/Charter
- Organizational ownership structure
- The position held by any individual claiming to act on behalf of a legal entity and a document confirming the powers of such individual
- Ownership and control structure of a legal entity as well as verification of the individuals who ultimately control the such legal entity
- The identity of the individuals who ultimately control the legal entity (see above)
- The list of key supervisors
- Deed of trust (if any)

- In the case of a partial fiduciary agreement, it must include the front page of the original fiduciary document and the last pages of the last fiduciary document, which should contain the following information:
  - Appointment of acting fiduciaries
  - Full name of the trust and conduct of business on behalf of, and
  - Fiduciary's signature (if any)
  - Trust declaration (if any)
  - Charter of the fund (if any)
  - Declaration of the fund (if any)

C. For other legal entities, additional documentation may be requested (as decided by NEO BANKERS) for verification:

- Latest annual report
- Partner agreement (complete)
- Partner agreement (partial) or the latest annual report
- Data from reliable open sources such as an extract from the listing exchange stock indicating that the Member is listed on the stock exchange in a FATF member country. The list of licenses that govern the activities of a legal entity (if any).
- A legal entity user is also obliged to provide links to the state online resources of the country of their registration, where it is possible to confirm the registration and valid licenses of the User as well as the presence of any litigation, criminal cases, fines from regulatory authorities etc.

V. VERIFICATION

A. Documents used to whitelist an account must be validated prior to whitelisting an account. Identity verification may require multi-factor authentication, multilayer security, and other controls to ensure verification of the User's identity based on their account or other factors.
B. The following examples of verification methods applied by NEO BANKERS are not an exhaustive list of documents that NEO BANKERS may require:

– Obtaining address confirmation such as a copy of a utility bill or a bank statement from the account holder
– Comparing identifying information with information available from a trusted third-party source
– Checking whether there is a logical correspondence between the provided identifying information such as the User's name, postal address, telephone number, date of birth and social security number/taxpayer registration number (logical check)
– Using sophisticated device identification (such as digital fingerprints or IP geolocation verification).
– Obtaining a notarized or certified copy of a birth certificate/passport/ID card of an individual to verify the identity

VI. REPORTS ON PERFORMED TRANSACTIONS AND ACTIVITIES

A. For the purposes of the Policy, a "suspicious transaction" means a transaction or attempted transaction made by the User that:
- raises a substantiated suspicion that it may be related to proceeds from criminal or other illegal activities regardless of the size of such transaction;
- performed in the circumstances of unusual or needless complexity;
- has no clear economic rationale or true purpose;
- also raises a substantiated suspicion that it may relate to the financing of terrorism-related activities.

B. The Service monitors suspicious transactions and other suspicious activity related to transactions with Electronic Units and virtual currencies.

C. Internal control is exercised through an internal monitoring system to intelligently detect suspicious activity. When suspicious activity is detected, NEO BANKERS' key management personnel will decide whether such transaction can be defined as a suspicious transaction or activity and whether any documents should be filed with the law enforcement authorities. NEO BANKERS reserves the right to report suspicious transactions or actions to the law enforcement authorities at its sole discretion without notifying the User.

D. NEO BANKERS will keep a copy of a complaint as well as all documentation received. Filing a complaint is confidential. No one, other than those involved in the investigation and reporting, should be notified of its existence. Under no circumstances should the parties involved in suspicious activity be notified of filing a complaint with the law enforcement authorities.

VII. RECORD SUPPORT

A. This Policy requires reasonable procedures to keep the records of the information used to verify the name, address and other identifying information provided by the User with the intention to perform transactions with Electronic Units and Virtual Currencies. The following steps are required in the accounting process:

- NEO BANKERS keeps a record of the identifying information provided by its Users
- In cases where NEO BANKERS relies on a document to verify identity, NEO BANKERS stores a copy of the document that clearly indicates the document type and any identifying information it may contain

NEO BANKERS also keeps records of the methods and results of any additional measures taken to verify the User's identity. NEO BANKERS will record any discrepancies in the received identifying information. All records of transactions and identification will be stored as long as necessary for the purposes of the TGE and in accordance with the applicable regulations.

B. All information received from the Users will be governed by NEO BANKERS' Privacy Policy.

VIII. CONTINUOUS MEASURES TAKEN BY NEO BANKERS

A. Cooperation only with those Electronic Payment Systems and other financial partners that have implemented the Policy for the Assessment and Management of Monetary and Terrorist Financing Risks.
B. Establishing and maintaining risk-based customer due diligence review, identification, verification and KYC procedures for the Users including enhanced due diligence review for the Users who pose a higher risk as politically exposed persons (PEPs) or public figures.
C. Procedures for reporting suspicious fraudulent use of identity documents to the relevant law enforcement authorities, as appropriate.
D. Maintaining appropriate records for the required period of time.
E. Providing appropriate management information and reporting personnel on compliance with the Policies to NEO BANKERS key management.
F. NEO BANKERS may require its Users to provide additional information or documentation in order to carry out legal checks and, when deemed appropriate, deny registration or performing a transaction for the User that is suspected of financial crime.

Customer Due Diligence (CDD) is one of the international standards for the prevention of illegal activities. For this purpose, NEO BANKERS implements its own verification procedures in compliance with the strict anti-money laundering standards and the "Know Your Customer" procedure. NEO BANKERS' identification procedure requires its User to provide NEO BANKERS with reliable, independent source documents, data or information (e.g., their national ID card, international passport, bank statement, utility bill). For such purposes, NEO BANKERS reserves the right to collect the User's identification information in order to comply with the AML/KYC Policy. NEO BANKERS will take steps to verify the authenticity of documents and information provided by the Users. NEO BANKERS will apply all legal methods for double-checking identity information; NEO BANKERS reserves the right to investigate the cases of certain Users who have been identified as dangerous or suspicious.

NEO BANKERS reserves the right to verify the identity of the Users on an ongoing basis, especially when their identification information has been changed or their activity seems suspicious (unusual for a particular User). In addition, NEO BANKERS reserves the right to request its Users to provide up-to-date documents even if they have already been authenticated in the past. User identification information will be collected, stored, shared and protected strictly in accordance with NEO BANKERS' Privacy Policy and related policies.

After confirming the identity of the User, NEO BANKERS may waive potential legal liability in a situation where the Company's services are used to conduct illegal activities.

Cryptocurrency and Virtual Asset Policy

This section outlines NEO BANKERS' policy regarding cryptocurrencies and virtual assets, in compliance with Regulation (EU) 2023/1114 (MiCA):

a) Definition of virtual assets and Virtual Asset Service Providers (VASPs):
Virtual assets are defined as digital representations of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual Asset Service Providers (VASPs) are entities that engage in exchange services between virtual assets and fiat currencies, transfer of virtual assets, safekeeping and administration of virtual assets or instruments enabling control over virtual assets, and participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

b) Registration/licensing requirements for VASPs:
NEO BANKERS shall ensure that it complies with all registration and licensing requirements as set forth in the MiCA regulation and any additional requirements imposed by Polish authorities. This includes obtaining necessary licenses, maintaining adequate capital requirements, and implementing robust governance structures.

c) Specific KYC/AML measures for cryptocurrency operations:
In addition to standard KYC/AML procedures, NEO BANKERS shall implement specific measures for cryptocurrency operations, including:
   - Enhanced due diligence for high-value crypto transactions
   - Monitoring of cryptocurrency wallet addresses for links to illicit activities
   - Implementation of travel rule requirements for crypto transfers
   - Regular risk assessments specific to crypto-related money laundering and terrorist financing risks

d) Transaction monitoring using blockchain analytics:
NEO BANKERS shall utilize advanced blockchain analytics tools to monitor transactions on various blockchains. This will help in identifying suspicious patterns, tracking the flow of funds, and detecting potential links to illicit activities.

e) Rules for cross-border transfers of virtual assets:
NEO BANKERS shall comply with the travel rule requirements as stipulated in the FATF recommendations and the MiCA regulation. This includes collecting and transmitting required information for cross-border virtual asset transfers above the designated threshold.
NEO BANKERS shall not process any transaction above 0.5 BTC or the equivalent in another cryptocurrency or fiat currency without complete User information or additional verification, in compliance with Article 115 of Regulation (EU) 2023/1114 (MiCA).

LEGAL POLICY

ANTI-MONEY LAUNDERING, COUNTER-TERRORISM FINANCING AND WEAPONS OF MASS DESTRUCTION PROLIFERATION PREVENTION POLICIES (AML/CTF)

AML Compliance Officer

The AML Compliance Officer is the individual duly authorized by NEO BANKERS responsible for ensuring the effective implementation and enforcement of the AML/KYC Policy. Such Officer is required to monitor all aspects of NEO BANKERS' anti-money laundering activities including money laundering and terrorist financing, including but not limited to the following methods:

- Collection of the User identification information
- Setting and updating the internal policies and procedures for the completion, review, submission and storage of all reports and records required by the applicable laws and regulations
- Monitoring transactions and investigating any significant deviations from normal activities
- Implementing a records management system for appropriate storage and retrieval of documents, files, forms and logs
- Regularly updating risk assessment measures
- Providing law enforcement agencies with the information they need to comply with the applicable laws and regulations

The AML Compliance Officer has the right to interact with the law enforcement agencies that are involved in preventing money laundering, terrorist financing and other illegal activities. The Users are verified not only by verifying their identity, but more importantly by analysing their transaction behaviour. Therefore, NEO BANKERS relies on data analysis as a risk assessment and suspicion detection tool. NEO BANKERS performs a variety of compliance tasks including data collection, filtering, record keeping, investigation management and reporting.

The system features include:

- Checking Users on a daily basis for the presence of recognized blacklists (for example, OFAC), aggregating transmissions across multiple data points, placing the Users on watchlists and denying certain services, starting investigatory cases where necessary, sending internal messages and completing mandatory reports, if applicable
- Management of affairs and documents

With regard to the AML/KYC policy, NEO BANKERS will monitor all transactions and reserves the right to:

- ensure that suspicious transactions are reported to the appropriate law enforcement agencies through the AML Compliance Officer
- request the User to provide any additional information and documents in the event of any suspicious transactions
- suspend or terminate the User's account if NEO BANKERS has a substantiated suspicion that such User is engaging in illegal activity.

The above list is not exhaustive and the AML Compliance Officer will monitor the Users' transactions on a daily basis to determine whether such transactions should be reported and considered suspicious. In accordance with international requirements, NEO BANKERS applies risk assessment practices to combat money laundering and terrorist financing. By applying risk assessment practices to combat money laundering, NEO BANKERS ensures that the measures intended to prevent or mitigate money laundering and terrorist financing are commensurate with the identified risks.

Policy Review and Update

This Policy shall be regularly reviewed and updated to ensure compliance with current Polish and EU legislation. The review process will take into account:

- Changes in applicable laws and regulations
- Feedback from regulatory authorities and auditors
- Emerging trends in money laundering and terrorist financing techniques
- Advancements in technology and their impact on AML/CFT measures
- Internal audit findings and recommendations

The above list is not exhaustive and the AML Compliance Officer will monitor the Users' transactions on a daily basis to determine whether such transactions should be reported and considered suspicious. In accordance with international requirements, NEO BANKERS applies risk assessment practices to combat money laundering and terrorist financing. By applying risk assessment practices to combat money laundering, NEO BANKERS ensures that the measures intended to prevent or mitigate money laundering and terrorist financing are commensurate with the identified risks.

The AML Compliance Officer is responsible for initiating and overseeing the review process. Any changes to the Policy must be approved by NEO BANKERS' senior management and communicated to all relevant staff members.

Revision date: August 12th, 2024.

We appreciate your time.
Respectfully, sincerely yours,

The NeoBankers team