PROCRYPTIC SP. Z O.O.

Anti-Money Laundering and Counter-Terrorist Financing Policy

(“Procryptic AML/CTF Policy”)

Version:	1
Produced	June 2023

1. INTRODUCTION

The purpose of this Procryptic AML/CTF Policy is to determine and to describe the procedures, policies, regulations and mechanisms which are established, implemented and maintained by Procryptic sp. z o.o. in compliance with the applicable legislation. The procedures are designed to establish, implement and maintain policies, controls and procedures to detect, manage and effectively counter and mitigate the money laundering and terrorist financing (hereinafter the "**ML/TF**")

Procryptic sp. z o.o. based in Warsaw (hereinafter the "**Company**") has been established by the Metafortune Limited to provide virtual currencies services in accordance with its entry in the Register of virtual currency activities (no. RDWW-83).

The Company it is obliged to operate in accordance with Polish legal provisions regarding ML/TF.

This document is designed strictly for internal use of the Company and its relevant persons. This document or any part of its contents could be disclosed and/ or made available to other persons, including auditors and supervisory authorities only in cases and on the conditions, which are prescribed by this document or by law.

Each employee is required to confirm in writing that he/she is familiar with this Procryptic AML/CTF Policy. The template of confirmation is attached as Appendix 1 to this Procryptic AML/CTF Policy.

Relevant Legislation and References:

- Act on Prevention of Money Laundering and Financing of Terrorism of 1 March 2018 (hereinafter the "**PL AML Act**")
- 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, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (hereinafter the "**Directive**")

The MLRO shall act as a person indicated in Article 8 of the PL AML Act - an employee responsible for overseeing the compliance of the Company with ML/TF provisions of law. The MLRO is also responsible for overseeing the compliance of the Company with ML/TF internal procedures and reporting.

2. RISK ASSESMENT

2.1. The Company identifies and assesses the ML/TF risks related to its activities, considering risk factors relating to clients, countries or geographical areas, products, services, transactions or their delivery channels in accordance with this Procryptic AML/CTF Policy, taking into consideration in particular:

2.1.1. Information on ML/TF made available to the Company by the applicable regulatory and governmental authorities (where relevant) and

2.1.2. With regards to each clients' risk factor defined in clause 2.5 - probability, the consequences of its realization and the probability of an increase in that risk.

2.2. The risk assessment referred to in point 2.1 is prepared and maintained in electronic form. The risk assessment is updated when necessary, but at least every 2 years, by the MLRO. The updates shall be made in particular, due to changes in risk factors concerning clients, countries or geographical areas, products, services, transactions or their delivery channels or amendments of the national risk assessment and European Commission report referred to in Article 6(1) to (3) of the Directive. The MLRO shall present the results of the risk assessment to the Board together with its recommendations for any required amendments to the Company's measures or procedures.

2.3. At the request of the Inspector General (Generalny Inspektor Informacji Finansowej – "GIIF"), Company is obliged to provide its risk assessment and other information that may have influence on the national risk assessment.

2.4. The Company identifies and assesses the ML/TF risks relating to its clients.

2.5. The Company takes into consideration in particular the following factors when assessing the ML/TF clients' risk:

a) type of client,

b) the geographical area,

c) purpose of the account,

d) the type of products, services and distribution methods,

e) amount of property values deposited by the client or the value of transactions carried out,

f) purpose, regularity or duration of the business relationship.

2.6. The Company takes into consideration the above and categorizes the Clients in accordance with this Procryptic AML/CTF Policy (as High, Standard or Low Risk Clients), taking into consideration the circumstances which may represent a higher or lower ML/TF risk specified in art. 42 and 43 of the PL AML Act and clauses 5 and 6 of this Procryptic AML/CTF Policy. Taking into consideration the assessed risk, the Company determines the type and extent of measures it adopts, to manage and mitigate the identified risks effectively in accordance with the Procryptic AML/CTF Policy.

2.7. The Company applies the following financial security measures shall include:

a) Client identification and verification of its identity (in accordance with p. 3);
b) beneficial owner's identification and taking reasonable actions for the purpose of:
    i. verification of his/her identity;
    ii. establishing of the ownership and control structure – in the case of a customer that is a legal person, organizational unit having no legal personality or a trust;
        - in accordance with p. 3.
c) the assessment of business relationships and, as appropriate, obtaining information on the purpose and intended nature of those relationships – in accordance with onboarding procedures in the Company and KYC form;
d) ongoing monitoring of the business relationships of the client, including:
    i. an analysis of transactions undertaken throughout the course of business relationships to ensure that the transactions are consistent with the Company's knowledge of the client, his/her business type and scope, and consistent with the ML/TF risk related to this client – in accordance with Appendix 2;

ii. investigation of the source of origin of property values at the disposal of the Client - in the cases justified by circumstances– in accordance with Appendix 3;
iii. ensuring that the documents, data or information on business relationships held are kept up-to-date – in accordance with Appendix 3.

2.8. The Company does not accept the following categories of Clients who are prohibited to enter into any type of business relationships with the Company:

a) Clients who do not provide sufficient documents and/ or information for establishment and verification of their identity, their ownership structure and beneficial owners,
b) Clients who fall under sanctions based on decisions of competent authorities of European Union, OFAC or other international organizations,
c) Citizens of some countries where activity of the Company is prohibited.

3. CLIENT ACCEPTANCE & DUE DILIGENCE (CDD)

3.1. The Company performs the process of clients' due diligence (CDD).

3.2. Clients' due diligence aims at identifying, in particular, in the case of:

3.2.1. a natural person:

a. name and surname,

b. nationality,

c. Public Electronic System for Registration of Population (PESEL) number or in cases where the person does not have PESEL - date of birth and country of birth,

d. series and no. of the document confirming identity (ID),

e. the address of residence - if the Company possess such information,

f. name (business name), Tax Identification Number (NIP) and address of the main place of business activity – applies to entrepreneurs.

3.2.2. a legal person:

a. name (business name),

b. legal entity type,

c. address of registered or business office,

d. Tax Identification Number (NIP), and if the client does not have NIP - country of registration, name of commercial register where the client is registered, registration number and date of registration,

e. identification data referred to in point 3.2.1 considering the person who act on behalf of the client.

3.3. The identification of the beneficial owner shall include the determination of the data referred to in point 3.2.1(a) and (b) and when the Company possess such information - also the data referred to in point 3.2.1 (c)-(e) of this Procryptic AML/CTF Policy.

3.4. The identification of a person authorized to act on behalf of the client includes identification of the data referred to in point 3.2.1(a)-(d) of this Procryptic AML/CTF Policy.

Identification of (1) the client being natural person, (2) beneficial owner or (3) person authorized to act on behalf of the client – required documents

3.5. Verification of Identity document involves verification of the type of presented document and checking if data provided by the client is the same as the data in the document. The following documents (IDs) are acceptable identity documents:

a. Identity card;

b. Passport;

c. Residence card,

provided that in case of a client being a citizen of a non-EEA country the Company shall obtain form this client a residence card or passport.

3.6. When verifying the ID, the employees check in particular:

a. if the document is valid,

b. if there are no doubts regarding its authenticity,

c. if personal data visible at the ID is the same as the data provided in the agreement (name, surname, date of birth, PESEL no. [if applicable]),

d. if the document is legible and the copy provided has not been subject to modification in particular if identification data remains unchanged.

3.7. Verification of additional document confirming the identity, involves verification of the type of presented document. The following additional documents are accepted:

a. Identity card (if not received pursuant to clause 3.5 as ID document);

b. Passport (if not received pursuant to clause 3.5 as ID document);

c. Residence card (if not received pursuant to clause 3.5 as ID document);

d. bank statement or other document related to banking activities (issued not earlier than within 3 months before the day of conclusion of an agreement);

e. driving license;

f. phone bill (issued not earlier than within 3 months before the day of conclusion of an agreement);

g. utility bill concerning the services provided periodically to the place of residence (issued not earlier than within 3 months before the day of conclusion of an agreement);

h. tax decision (issued not earlier than within 12 months before the day of conclusion of an agreement);

i. government document (issued not earlier than within 12 months before the day of conclusion of an agreement);

j. student or doctoral ID (valid on the day of agreement conclusion);

k. registration certificate (valid on the day of agreement conclusion).

3.8. The Company shall collect and verify at least one identification document (clause 3.5) in addition to at least one additional identification document as specified above in clause 3.7.

Identification of legal persons and organizational units without legal personality – required documents

3.9. Appropriate identification of the legal person or organizational entity, in particular in case of entity entered to the National Court Register (KRS), requires obtaining:

a. original or copy of current extract from the relevant register - if the entrepreneur's data is available in the eKRS or other public registers of entrepreneurs, the employee can add printouts from the abovementioned registers to the client's documentation,

b. original or copy of certificate on the award of statistical REGON number in case of Polish entrepreneurs. If the REGON number is included in the extract above it is not necessary to provide REGON certificate. If the REGON number is not included in the extract from a relevant companies register, the employee can download the certificate from the Internet on its own and add it to the client's documentation,

c. original or copy of certificate of the award of relevant tax identification number. If, in case of Polish entrepreneurs, the NIP number is included in the extract form KRS, then the printout mentioned in point a) is sufficient. If the NIP number is not included, the employee can download the certificate from the Internet on its own and add it to the client's documentation,

d. list of beneficial owners including their names, surnames, addresses of residence, PESEL numbers or dates of birth - if no PESEL number was awarded, and countries of birth, copy of identity cards or passports of such beneficial owners,

e. printout from Central Register of Beneficial Owners (Centralny Rejestr Beneficjentów Rzeczywistych), if applicable,

f. name, surname, citizenship, PESEL number or date of birth (if PESEL number was not awarded), and country of birth, copy of the identity card or passport of persons authorized to represent the client,

g. copy of certificate issued by the bank or bank account statement containing corporate data and address details compliant with data provided in the agreement.

3.10. The true translation must be provided in the event when the documents provided are not in Polish or English.

3.11. The Company may request additional information and documents in accordance with the AML/CTF Policy.

3.12. The verification of the client's/beneficial owner's identity has to be completed before entering into a commercial relationship in particular before accepting the client and before conduction occasional transaction.

3.13. CDD shall also be made when the Company performs an occasional transaction:

a. with the value equivalent to EUR 15,000 or more, irrespective of whether the transaction is conducted as a single operation or as several operations which seem to be linked, or

b. which constitutes the transfer of funds for the amount exceeding EUR 1,000,

c. using virtual currencies equivalent to EUR 1,000 or more,

and when the Company suspects ML/TF or has doubts on the veracity or adequacy of documents or information previously obtained for identification or verification.

3.14. The verification of the identity of the client and the beneficial owner may be completed by the Company at the start of the business relationship where this is necessary to ensure the continuity of the business and there is a low risk of ML/TF. In such cases, the verification shall be carried out as soon as possible after commence of business relationship.

3.15. The Company may conclude an agreement with and open client's account, allowing the client to trade, provided that the financial security measures described herein are applied.

3.16. Prior to start of business relationships or prior execution of occasional transaction, the Company shall inform the client about processing his/her personal data, in particular about the duties of the Company set forth under the PL AML Act to the extent of the data processing.

4. CENTRAL REGISTER OF BENEFICIAL OWNERS (CRBR)

4.1. Discrepancies between information gathered during the CDD process and information from the Central Register Of Beneficial Owners (*pl. Centralny Rejestr Beneficjentów Rzeczywistych* – "CRBR") as well as impediments identified in connection with verification of the identity of the beneficial owner and actions taken in connection with the identification of an individual in a senior management position as the beneficial owner shall be reported to the MLRO.

4.2. Each discrepancy mentioned in clause 4.1 shall be documented in the Company's CRM system in a form of a short note.

4.3. The Company takes steps to resolve the reasons for the discrepancies by contacting the client via email and/or telephone. If the discrepancies are confirmed, the Company shall provide the competent authority in charge of the CRBR with verified information on these discrepancies, together with the justification and documentation of the identified discrepancies.

4.4. This clause 4 applies only to the clients subject to registration with the CRBR (i.e. to Polish commercial companies).

5. SIMPLIFIED FINANCIAL SECURITY MEASURES

5.1. The Company may apply simplified financial security measures in the cases in which the risk assessment referred to in clause 2.4 confirmed a lower risk of ML/TF.

5.2. A lower ML/TF risk can be indicated in particular by:

5.2.1. the fact that the Client is:

a) a public finance sector entity referred to in Article 9 of the Act of 27 August 2009 on the Public Finance;
b) a state enterprise or a company with a majority shareholding of the State Treasury, territorial self-government units or their unions;

c) a company, the securities of which are admitted to trading on a regulated market subject to the requirements of disclosure of the information on its beneficial owner resulting from the provisions of the European Union law or the provisions of a third country corresponding thereto, or a company with a majority shareholding of such a company;
d) a resident of a Member State;
e) a resident of a third country defined by reliable sources as a country of low corruption or other criminal activity levels;
f) a resident of a third country in which, according to the data from reliable sources, the provisions concerning AML/CTF are applicable, which provisions correspond to the requirements under the regulations of the European Union in the field of AML/CTF;

5.2.2. the fact of offering products or services for the purpose of ensuring an appropriately defined and limited access to financial system for the clients having limited access to products or services offered as part of this system;

5.2.3. the fact of offering products or services related to a customer, in the case of which products or services the ML/TF risk is mitigated by other factors, including by participation units of open-end investment funds or specialized open-end investment funds or specific types of electronic money;

5.2.4. the fact of linking business relationships or an occasional transaction with:

a) a Member State;
b) a third country defined by reliable sources as a country of low corruption or other criminal activity levels;
c) a third country in which, according to the data from reliable sources, the provisions concerning combating money laundering or terrorist financing are applicable, which provisions correspond to the requirements under the regulations of the European Union in the field of combating money laundering and terrorist financing.

5.3. Simplified financial security measures shall not apply in the cases referred to in clause 3.13.

6. ENHANCED FINANCIAL SECURITY MEASURES

6.1. The Company shall apply enhanced financial security measures in the following cases:

6.1.1. the Company identified any of the indicators of higher risk of ML/TF as per clause 6.2,

6.1.2. commencement of business relationships or conducting transactions related to a high-risk third country identified by the European Commission in a delegated act adopted under Article 9 of Directive 2015/849,

6.1.3. the Company identified client or beneficial owner as PEP.

6.2. A higher risk of ML/TF can be indicated in particular by:

a) establishment of business relationships in unusual circumstances;
b) the fact that the client is:

i. a legal person or an organizational unit having no legal personality, whose activity serves to storage of personal assets;
ii. a company in which bearer shares were issued, whose securities are not admitted to organized trading, or a company in which the rights attached to shares or stocks are exercised by entities other than shareholders or stockholders;
iii. a resident of the state referred to in point g;

c) the subject of the business activity carried out by the client covering conducting of a significant number of cash transactions or cash transactions of high amounts;
d) unusual or excessively complex ownership structure of the client, having regard to the type and scope of the business activity conducted by this client;
e) the fact of the client making use of services or products offered as part of private banking;
f) the fact of the client making use of services or products contributing to anonymity or hindering the client's identification;
g) the fact of establishment or maintenance of business relationships or conducting an occasional transaction without the client being physically present – in the case when a higher risk of ML/TF related thereto was not limited in another manner;
h) the fact of ordering of transactions by third entities unknown or not linked to a client, the beneficiary of which transactions is the client;
i) the fact of covering by business relationships or transactions of new products or services or offering of products or services with the use of new distribution channels or new technological solutions;
j) linking business relationships or an occasional transaction with:
i. a high-risk third country;
ii. a country defined by reliable sources as a country of high corruption or other criminal activity levels, a country providing funding or support for committing activities of a terrorist nature, or with which an activity of an organization of a terrorist nature is associated;
iii. a country in relation to which the United Nations Organization or the European Union have taken a decision on imposing sanctions or specific restrictive measures;
k) the fact that business relationships or occasional transaction are related to crude oil, arms, precious metals, tobacco products, cultural artefacts, ivory, protected species or other items of archaeological, historical, cultural and religious importance, or of rare scientific value;
l) the fact that business relationships or occasional transaction are related to a client who is a citizen of a third country and applies for a right to stay or citizenship in a Member State in exchange for capital transfers, immovable property acquisition or Treasury bonds or, as the case may be, investments in corporate entities in a given Member State.

6.3. The Company carries out an ongoing analysis of the transactions being conducted.

6.4. In the case of disclosure of the following transactions:

a) complex or

b) of high amounts, which are not justified by the circumstances of conducting transactions; or

c) conducted in an unusual manner; or

d) which seem not to have legal or business grounds

– the Company takes actions in order to explain the circumstances in which these transactions were conducted and, in the event of transactions conducted as part of business relationships, the Company intensifies the application of the financial security measure referred to in clause 3 in relation to the business relationships as part of which these transactions were conducted.

6.5. In the case when a Client's transaction involves a high risk of ML/TF, in addition to applying the enhanced financial security measures, the Company:

a. take additional actions as part of enhanced financial security measures;
b. implement enhanced obligations relating to the reporting of information or transaction reporting;
c. limit the scope of business relations or transactions.

6.6. The MLRO shall be informed on the transaction described in clause 6.5. MLRO decides which action referred to in clause 6.5 shall be applied and gives precise guidelines what measures shall be taken.

6.7. The Company abide a decision of GIIF ordering a change in the scope or termination of correspondent relationships or a review of correspondent relationships with a respondent institution located in a High-risk third country.

7. RECORD-KEEPING AND ML/TF REPORTING TO PUBLIC AUTHORITIES

7.1. The activities described in this Procryptic AML/CTF Policy shall be appropriately documented by the Company.

7.2. The Company shall keep the documents and records in electronic form using the CRM System and in hardcopies in lockable cabinets. The MLRO shall supervise the process of record keeping. The documents and records shall be made available without delay to GIIF.

7.3. The Company is obliged to provide the GIIF with information mentioned in Art. 72, 86 and 90 of the PL AML Act i.e.:

a. Within 7 days of the occurrence of event, the Company shall send information on:

i. accepted payment or withdrawal of funds in cash the value of which exceeds an equivalent of EUR 15,000;

ii. transaction of foreign currency purchase or sale, when such transaction exceeds the equivalent of EUR 15,000, or information on being an intermediary of such transaction.

b. Immediately - information on having a reasonable suspicion that a particular transaction or assets may be related to ML/TF.

c. Immediately - information on execution of the transaction mentioned in point b - in case when GIIF could not be notified prior to its execution. In the notification the Company shall justify the reasons why the information was not provided prior execution and information available to the Company justifying the suspicion of ML/TF.

7.4. The reports mentioned in clause 7.3(a) will be prepared in .xml using the schemes published in the Central Repository for Electronic Documents (http://crd.gov.pl/). The no. of appropriate schemes may be checked under: https://www.gov.pl/web/finanse/komunikaty-giif The reports will be send throughout the GIIF system - https://www.giif.mofnet.gov.pl/ .

7.5. The reports mentioned in clause 7.3(b) and (c) will be send via email or ePUAP.

7.6. The Company notifies the relevant prosecutor without delay if has a reasonable suspicion that property values being the subject of transaction or kept on the account originate from or relate to a fiscal offence or any offence other than ML/TF (SAR). The notification shall be made in accordance with Article 89 of the PL AML Act i.e. shall contain information available to the Company that gave rise to the suspicion and information about the expected time of the transaction. Until receipt of the prosecutor's decision to initiate or refuse to initiate proceedings, the time shall not exceed 96 hours from the time of sending the notice, the Company shall refrain from carrying out the reported transaction, or any other transactions which may debit client's account.

7.7. In case when a notification could not be made before execution of transaction referred to in clause 7.6 the Company immediately notify the relevant prosecutor that the transaction has been executed. In its notification the Company shall justify the reasons why the transaction was not reported earlier and the information available to the Company justifying the suspicion of ML/TF.

7.8. The Company shall inform the GIIF of circumstances that may indicate a suspicion of ML/TF.

7.9. The Company shall notify the GIIF of any circumstances which may indicate a suspicion that ML/TF criminal offence has been committed.

7.10. At the request of GIIF or prosecutor the Company shall freeze assets, suspend a transaction or block client's account.

7.11. Frozen funds under financial sanctions legislation and any case in which the Company has knowledge or a reasonable suspicion that the financial sanctions measures have been or are being contravened, or that a client is a listed person or entity, or a person acting on behalf of a person or entity subject to financial sanctions must be reported to the applicable authority.

7.12. At no point will the client, any of its representatives, or any third parties (excluding parties to which a report is to be made under this part or any applicable law), be informed about the suspicion arising hereunder, or any report made in connection therewith.

7.13. SARs will be prepared and retained within the Suspicious Activity Reporting subfolder within the Compliance folder. An additional subfolder will hold the Filed SARs. That file will include the csv transaction file and SAR narrative described below, and a copy of the email acknowledgment from the GIIF.

8. INTERIAL CONTROL AND INTERNAL REPORTING OF ML/TF VIOLATIONS

8.1. Compliance of the Company's activity with the regulations on ML/TF as well as this Procryptic AML/CTF Policy is subject to internal control made by the Company's Compliance Officer. The control shall be made at least once a year.

8.2. Every employee has the right to report actual or potential ML/TF violations. The report shall be sent in accordance with the Whistleblowing Procedure, attached as Appendix 5 to this Procryptic AML/CTF Policy.

8.3. The fact of notifying GIIF or other competent authorities in accordance with the PL AML Act and information on the analyses conducted regarding ML/TF shall be kept in secret.

9. POLITICALLY EXPOSED PERSON (PEP)

9.1. The Company has adopted and complies with Politically Exposed Persons Procedure attached as Appendix 4 to this Procryptic AML/CTF Policy ("**PEP Procedure**")

9.2. The list of national public positions and functions which are politically exposed positions is introduced in the regulation of the Ministry of finance and in the Exhibit A to the PEP Procedure.

9.3. In the case of business relationships with a PEP, the Company applies the following CDD measures and undertake the following activities in relation to such persons: 1) obtain the permission of the BoD for establishing or continuation of business relationships with a PEP; 2) applies adequate measures in order to establish the source of the client's wealth and sources of assets available to the client under the business relationship or the occasional transaction – in accordance with EDD procedures.

10. PROCRYPTIC AML/CTF POLICY IMPLEMENTATION AND TRAININGS

10.1. The MLRO will conduct at least once a year ML/TF training for all employees of the Company. In addition, every Company's new employee should receive training in the first days of its work.

10.2. This Procryptic AML/CTF Policy, prior to its implementation, shall be approved by the BoD of the Company.

APPENDIX 1
Template of confirmation - procedures

OŚWIADCZENIE **o zapoznaniu się z procedurami obowiązującymi w Procryptic Spółka z ograniczoną odpowiedzialnością w Warszawie („Spółka")**	***STATEMENT*** ***on familiarizing with the procedures implemented in Procryptic Spółka z ograniczoną odpowiedzialnością w Warszawie ("Company")***
Ja niżej podpisany/a oświadczam, że zapoznałem/am się z następującymi procedurami obowiązującymi w Spółce: 1. Anti-Money Laundering and Counter-Terrorist Financing Policy	*I, the undersigned, hereby declare that I have familiarized myself with the following procedures implemented in the Company:* *1. Anti-Money Laundering and Counter-Terrorist Financing Policy*
Oświadczam też, że zrozumiałem wyżej wymienione procedury i zobowiązuję się ich przestrzegać.	*I also declare that I have understood the above-mentioned procedures and undertake to follow them.*

Imię i nazwisko*/Name and Surname*	
Dział*/Department*	

Warszawa, data*/date*: ____/____/_____

Podpis*/Signature*:

APPENDIX 2
Analysis of transactions undertaken throughout the course of business relationships

Ongoing Monitoring is the periodic review of the Client relationship. The frequency of this periodic review will be determined in accordance with the Client's Risk Profile, which is identified during the onboarding process.

Clients escalated for Ongoing Monitoring will be added to the Ongoing Monitoring Log in a separate tab corresponding to their initial Risk Profile. When a Client is reviewed, findings of each review will be logged in the Ongoing Monitoring Log.

Any documentation collected will be stored in the relevant file within the applicable subfolder of the Compliance folder. The Company analyze the transactions undertaken by the Clients throughout the course of business relationships using FUGU for FIAT transactions and Chainanalysis for Crypto transactions.

- Updating Client Details, and Repeating the CDD:

In an effort to keep the details, information, and documentation of Clients updated and accurate at all times the MLRO will repeat the Client Due Diligence (CDD) process during the monitoring periods listed below. If doubt arises in the course of the business relationship regarding any of the details obtained during onboarding, the relevant queries and reviews will be repeated, and the relevant details will be updated.

Low Risk Clients (every 24 months)
- Screen client details
- Screen overall transaction activity

Standard Risk Clients (every 18 months)
- Screen client details
- Screen overall transaction activity

High Risk Clients (every 12 months)
- Screen client details
- Screen overall transaction activity
- Include synopsis in annual report to Chief Compliance Officer

As stated above, the results of all reviews will be logged in the Ongoing Monitoring Log for each Client reviewed. Any Client who needs a change to their Risk Profile will be escalated to the BoD for approval with a written recommendation. Any documentation collected from a Client will be stored within the subfolder corresponding to their review period.

APPENDIX 3
Investigation of the source of origin of property values at the disposal of the Client

The source of funds review will consist of:

- First considering the prima facie legitimacy of the Client's source of funds.
- Next, reviewing the client's jurisdiction risk and Client Risk Profile.
- Third, conducting a blockchain analysis of the Client's wallet address(es), where applicable or using third party service provider for fiat transaction review (including monitoring and screening).
- Finally, for very high sums (anything above EUR 1000) requesting additional information from the Client if additional high risk red flags are noted.

The reviewer should be able to identify what the destination address for the outgoing funds (blockchain) is via a block explorer or Chainalysis Reactor.

The reviewer should note what the wallet is composed of for incoming funds, i.e. funds from an exchange, high risk market, gambling etc, using Chainalysis Reactor.

Review the user's account in the Company's CRM system:

- Transaction history and test transactions.
- IP Address (in User Action Logs)/Location and device history.
- Referral source, or accounts referred if any.
- Onboarding documents and notes.
- Finally, review any notes added to the CRM system.

APPENDIX 4
PEP Procedure

I. SUMMARY

The objective of this document is to outline the procedure on the acceptance, management and monitoring of clients which are considered to be Politically Exposed Persons ("**PEPs**"). This is done to mitigate reputational risk, operational risk, regulatory risk and legal risks, based on internationally accepted best practices, standards and guidelines on the management of PEPs.

II. DEFINITIONS

Politically Exposed Persons
PEPs are persons entrusted with a prominent public function (as well as their families and persons known to be close associates) other than as a middle ranking or more junior official.

The list of national public positions and functions which are PEPs is introduced in the regulation of the Ministry of finance and in the Exhibit A to this PEP Procedure.

Family members of PEPs include:

- their spouse or partner;
- their and their spouse' or partner's children; and
- their parents.

Known close associates of a PEPs include:

- an individual who is known to have joint beneficial ownership of a legal entity or legal arrangement, or any other close business relations, with a PEP; and
- an individual who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the benefit of a PEP.

PEPs, their families and any close associates, are subject to enhanced scrutiny, because they may be in a position to abuse their public office for private gain by either misusing public funds or accepting bribery and corruption.

Accordingly, the Company shall screen all of Company's clients upon onboarding against known PEP lists, to verify their PEP status.

Clients who are PEPs are classified as Special Category Client ("**SCC**") (High Risk profile score), and are subject to specific enhanced due diligence ("**EDD**") measures, including increased monitoring and lower threshold limits. Company's accounts for PEPs may only be opened with the approval of the Company's Compliance Officer in addition to other approvals as required under this procedure.

III. IDENTIFICATION OF PEPs

The Company is not precluded from doing business with a PEP, and therefore the identification of a PEP does not on its own create an automatic reason to decline or reject an application for an

account/digital wallet. However, when a PEP is identified, Enhanced Due Diligence (EDD) should be conducted prior to a decision on whether to establish a business relationship or not.

Identification of a PEP

The Company identifies PEPs by:

- Screening clients against identified PEP lists
- Risk profiling a client as a PEP from communications with the client
- Considering other reputable sources of information such as industry publications, government publications or press releases

In order to identify client or beneficial owner as PEP the Company, the Company may accept a written or documentary declaration from the client that he/she is or is not a politically exposed person. The declaration has to be made under penalty of criminal liability for making a false declaration. The declaration shall contain the following statement: "I am aware of the criminal responsibility for making a false statement" – which replaces the instruction on criminal liability for making a false declaration.

Entities in which a PEP has beneficial interest or control

In the event that a PEP is an associated party to an entity and holds more than 25% voting rights in the entity, the entity itself will be regarded as high risk due to the association with a PEP. The PEP designation stems from the beneficial owner, shareholder, or controller and is not driven by the entity itself.

An entity should also be considered as high risk if significant influence over the policy, business and strategy of that entity is performed by a PEP. To determine if a PEP exercises significant influence over the policy, business and strategy of an entity, consideration needs to be had as to the nature of the position held by the individual concerned.

IV. KNOW YOUR CUSTOMER (KYC) REQUIREMENTS

Identification and Identification process

For each new business relationship, KYC information should be obtained during the on-boarding process and when accessing potential opportunities. This information will be used by the Company to conduct background screening on the client.

Client facing employees are required to make sure that the correct information is obtained from clients as per the applicable KYC checklists.

Pre-approval – Customer Due Diligence (CDD)

CDD is the key and primary source of information used for determining whether a customer is a PEP or not. CDD must be conducted when:

- Establishing a business relationship with a client
- At regular intervals during the lifecyle of the client, based on the risk rating

- When there is a valid reason to doubt the authenticity of information or documentation or data or other information previously obtained for the purpose of KYC in question
- When otherwise required under Company's procedures

When conducting CDD on PEPs, beneficial owners may be uncovered and will be verified accordingly by the Compliance Function.

When there is a positive identification of a PEP, the Compliance Function will ensure that EDD is conducted.

Post approval discovery – CDD

If any employee uncovers that a client is a PEP during the day-to-day activities as and when they perform an activity on the client's account, the employee is required to inform the Compliance Function.

If there are any changes in the shareholding structure of a client, the new shareholder/s must be sent to the Compliance Function in order to conduct CDD and EDD if necessary, and the PEP registry will be updated accordingly.

V. TREATMENT of PEPs

In making the decision to approve or not approve an application when a PEP has been identified, the review will take into consideration all information discovered during the discovery of the PEP.

VI. PRE-APPROVAL DISCOVERY PROCESS

The following is a step-by-step illustration of the process to be followed when a PEP has been identified in the CDD process prior to approval:

1) When a PEP, family member, or associate has been discovered/identified during the CDD stage, responsible employee must send information to the Compliance Function.
2) The MLRO should perform a risk assessment of the PEP's proposed relationship. The risk assessment should be a composite of all the risk factors to determine if the proposed relationship with the PEP is of higher risk.
3) The following should be considered when conducting an assessment:
   a) Client risk factors, including geographic;
   b) Nature of PEP; and
   c) The products the PEP is seeking access to.
4) If the risk assessment establishes the proposed relationship presents a low risk, the MLRO will classify it accordingly and a less stringent EDD will be conducted.
5) If the risk assessment suggests that the proposed relationship with the PEP will be of high risk, the MLRO will have to ensure continuous monitoring of that account.
6) EDD will compromise the following:
   a) Seeking more information from the PEP for proposed of identifying and verifying whether there are any other beneficial owners;
   b) Seeking more information as to the proposed use of the account;
   c) Seeking verification on the source of funds, source of wealth.

7) Once EDD has been concluded, the MLRO will complete a summary including all relevant information discovered regarding the identified PEP. Such summary will be provided to the BoD.
8) Pursuant to FATF recommendations and applicable regulations in Poland, the BoD approval is required for establishing or conducting an existing business relationship with PEPs.
9) The MLRO will review the PEP and, if necessary, bring to the Board's attention to seek approval:
10) If the Board approves, then the business unit will be informed and the client will be able to enter a relationship with the Company;
11) If the Board rejects, then the business unit will be informed and the relevant processes will be followed for all rejected applications.

Exhibit A to the PEP Procedure
The list of national (Polish) public positions and functions which are politically exposed positions

1. President of the Republic of Poland;
2. Chairman of the Council of Ministers;
3. Vice-President of the Council of Ministers;
4. minister;
5. secretary of state;
6. undersecretary of state;
7. deputy;
8. senator;
9. member of the European Parliament;
10. member of a body representing a political party externally, entered in the register of political parties kept by the District Court in Warsaw;
11. member of a governing body of a political party entered in the register of political parties kept by the District Court in Warsaw, authorised to incur financial liabilities;
12. judge of the State Tribunal;
13. judge of the Supreme Court;
14. judge of the Constitutional Court;
15. judge of the Supreme Administrative Court;
16. judge of the Court of Appeal;
17. President of the National Bank of Poland;
18. member of the Management Board of the National Bank of Poland;
19. member of the Monetary Policy Council;
20. an authorized representative of the Republic of Poland in another country or at an international organization;
21. chargés d'affaires;
22. an officer who occupies an official position in the Armed Forces of the Republic of Poland ranked up to the rank of general (admiral);
23. a representative of the Minister of National Defence appointed on the basis of a separate decision of the Minister of National Defence;
24. director, president of a state enterprise or other equivalent position;
25. chairman of the supervisory board of a state enterprise;
26. member of the supervisory board of a state enterprise;
27. president of the management board of a company with State Treasury shareholding, in which more than half of the shares belong to the State Treasury or other state legal persons;
28. Board member of a company with State Treasury shareholding, in which more than half of the shares belong to the State Treasury or other state legal persons;
29. chairman of the supervisory board of a company with State Treasury shareholding, in which more than half of the shares belong to the State Treasury or other state legal persons;
30. supervisory board member of a company with State Treasury shareholding, in which more than half of the shares belong to the State Treasury or other state legal persons;
31. director general of the office of the chief state authority;

32. director general of the office of the central state authority;
33. director general of the provincial office;
34. Head of the Chancellery of the President of the Republic of Poland;
35. Head of the Chancellery of the Prime Minister;
36. Head of the Chancellery of the Parliament (Sejm);
37. Head of the Chancellery of the Senate;
38. voivode;
39. deputy voivode;
40. marshal of the province;
41. member of the board of the province other than the marshal of the province;
42. mayor of a village, mayor, president of a city;
43. deputy mayor of a village, mayor or president of a city;
44. starost;
45. member of the county board other than the starost;
46. Director General of the National Center for Agricultural Support;
47. Deputy Director General of the National Center for Agricultural Support;
48. General Director of the State Forests;
49. Deputy Director General of State Forests;
50. Director General of the Prison Service;
51. Deputy Director General of the Prison Service;
52. Director General of the Foreign Service;
53. Director General of the Office of the Chairman of the Committee constituting the Council of Ministers;
54. Director of the National School of Public Administration;
55. Deputy Director of the National School of Public Administration;
56. Director of the Polish Centre for Accreditation;
57. Deputy Director of the Polish Accreditation Centre;
58. Director of the Government Centre for Security;
59. Deputy Director of the Government Centre for Security;
60. Director of the Transport Technical Supervision;
61. Deputy Director of Transport Technical Supervision;
62. General Director of National Roads and Motorways;
63. Deputy General Director of National Roads and Motorways;
64. General Director of Environmental Protection;
65. Deputy General Director for Environmental Protection;
66. General Inspector of Financial Information;
67. Chief Geodesist of the Country;
68. Deputy Chief Geodesist of the Country;
69. Chief Pharmaceutical Inspector;
70. Deputy Chief Pharmaceutical Inspector;
71. Chief Inspector of Trade Quality of Agricultural and Food Products;
72. Deputy Chief Inspector of Trade Quality of Agricultural and Food Articles;
73. Chief Inspector of Construction Supervision;
74. Deputy Chief Inspector of Building Supervision;
75. Chief Inspector of Plant and Seed Protection;
76. Deputy Chief Inspector of Plant and Seed Protection;
77. Chief Inspector of Environmental Protection;
78. Deputy Chief Inspector of Environmental Protection;
79. Chief Labour Inspector;
80. Deputy Chief Labour Inspector;
81. Chief Sanitary Inspector;
82. Deputy Chief Sanitary Inspector;
83. Chief Inspector of Road Transport;
84. Deputy Chief Inspector of Road Transport;
85. Chief Veterinary Doctor;
86. Deputy Chief Veterinary Doctor;
87. Chief Ombudsman for Financial Discipline;

88. Deputy Chief Ombudsman for Financial Discipline;
89. Chief Commandant of the State Fire Service;
90. Deputy Chief Commandant of the State Fire Service;
91. Commander-in-Chief of the Police;
92. Deputy Chief Commander of the Police;
93. Commander-in-Chief of the Border Guard;
94. Deputy Chief Commandant of the Border Guard;
95. Commander of the State Protection Service;
96. Deputy Commandant of the State Protection Service;
97. Chief Director of the State Archives;
98. Deputy of the Supreme Director of the State Archives;
99. President of the Military Property Agency;
100. Deputy President of the Military Property Agency;
101. President of the Agency for Restructuring and Modernization of Agriculture;
102. Deputy President of the Agency for Restructuring and Modernization of Agriculture;
103. President of the Bureau for Chemical Substances;
104. President of the Central Office of Measures;
105. Vice-President of the Main Office of Measures;
106. President of the Central Statistical Office;
107. Vice President of the Central Statistical Office;
108. President of the Institute of National Remembrance - Commission for the Prosecution of Crimes against the Polish Nation;
109. Deputy President of the Institute of National Remembrance - Commission for the Prosecution of Crimes against the Polish Nation;
110. President of the Agricultural Social Insurance Fund;
111. Deputy President of the Agricultural Social Insurance Fund;
112. President of the National Property Stock;
113. Deputy President of the National Property Stock;
114. President of the Supreme Chamber of Control;
115. Vice President of the Supreme Audit Office;
116. member of the College of the Supreme Audit Office;
117. President of the National Health Fund;
118. Deputy President of the National Health Fund;
119. President of the State Water Management Company Polish Waters (Wody Polskie);
120. Deputy President of the State Water Management Company Polish Waters (Wody Polskie);
121. President of the State Atomic Energy Agency;
122. Vice President of the State Atomic Energy Agency;
123. President of the Polish Space Agency;
124. Vice-president of the Polish Space Agency;
125. President of the Polish Audit Supervision Agency;
126. Deputy President of the Polish Audit Supervision Agency;
127. President of the Polish Agency for Enterprise Development;
128. Deputy President of the Polish Agency for Enterprise Development;
129. President of the Polish Tourist Organization;
130. Vice President of the Polish Tourist Organization;
131. President of the General Prosecutor's Office of the Republic of Poland;
132. Vice President of the General Prosecutor's Office of the Republic of Poland;
133. President of the Government Legislation Centre;
134. Vice President of the Government Legislation Centre
135. President of the Government Strategic Reserve Agency;
136. Deputy Chairman of the Government Strategic Reserves Agency;
137. President of the Office of Technical Inspection;
138. Vice President of the Office of Technical Inspection;
139. President of the Office of Electronic Communications;
140. Deputy President of the Office of Electronic Communications;
141. President of the Office of Civil Aviation;
142. Vice-President of the Civil Aviation Office;

143. President of the Office for Personal Data Protection;
144. Deputy President of the Office for Personal Data Protection;
145. President of the Office for Competition and Consumer Protection;
146. Vice-President of the Office for Competition and Consumer Protection;
147. President of the Patent Office of the Republic of Poland;
148. Deputy President of the Patent Office of the Republic of Poland;
149. President of the Energy Regulatory Office;
150. Vice President of the Energy Regulatory Office;
151. President of the Office for Registration of Medicinal Products, Medical Devices and Biocidal Products;
152. Vice President of the Office for Registration of Medicinal Products, Medical Devices and Biocidal Products;
153. President of the Office of Railway Transport;
154. Vice-President of the Railway Transport Office;
155. President of the Public Procurement Office;
156. Vice-president of the Public Procurement Office
157. President of the Higher Mining Office;
158. Vice President of the State Mining Authority;
159. President of the Social Insurance Institution;
160. member of the Board of the Social Insurance Institution;
161. President of the Management Board of Bank Gospodarstwa Krajowego;
162. Vice-President of the Management Board of Bank Gospodarstwa Krajowego
163. member of the Management Board of Bank Gospodarstwa Krajowego;
164. President of the Management Board of the National Fund for Environmental Protection and Water Management;
165. Deputy President of the Management Board of the National Fund for Environmental Protection and Water Management;
166. President of the Management Board of the State Fund for Rehabilitation of Disabled Persons;
167. Deputy President of the Management Board of the State Fund for Rehabilitation of Persons with Disabilities;
168. Attorney General;
169. Deputy Prosecutor General;
170. National Prosecutor;
171. Chairman of the Financial Supervision Commission;
172. Deputy Chairman of the Financial Supervisory Commission;
173. member of the Financial Supervisory Commission;
174. Chairman of the State Commission to clarify cases of acts against sexual freedom and morality against a minor under 15 years of age;
175. member of the State Commission for clarification of cases of actions directed against sexual freedom and morality against a minor under 15 years of age;
176. Chairman of the National Broadcasting Council;
177. Deputy Chairman of the National Broadcasting Council;
178. member of the National Broadcasting Council;
179. Chairman of the State Election Commission;
180. Deputy Chairman of the State Election Commission;
181. member of the State Election Commission;
182. Chairman of the Council for Refugees;
183. Vice-Chairman of the Council for Refugees;
184. Chairman of the National Media Council;
185. member of the National Media Council;
186. Financial Ombudsman;
187. Deputy Financial Ombudsman;
188. Ombudsman for Small and Medium Enterprises;
189. Deputy Ombudsman for Small and Medium Enterprises;
190. Ombudsman for Children;
191. Deputy Ombudsman for Children;
192. Ombudsman;
193. Deputy Ombudsman;

194. Ombudsman for Patients' Rights;
195. Deputy Ombudsman for Patients' Rights;
196. Head of the Internal Security Agency;
197. Deputy Head of the Internal Security Agency;
198. Head of the Intelligence Agency;
199. Deputy Head of the Intelligence Agency;
200. Head of the National Security Bureau;
201. Deputy Chief of the National Security Bureau;
202. Head of the Central Anti-Corruption Bureau;
203. Head of the National Election Office;
204. Head of the National Fiscal Administration;
205. Deputy Head of the National Fiscal Administration;
206. Head of the Civil Service;
207. Head of the Military Counterintelligence Service;
208. Deputy Chief of the Military Counterintelligence Service;
209. Chief of the Military Intelligence Service;
210. Deputy Chief of the Military Intelligence Service;
211. Chief of the Foreign Service;
212. Head of the Office for Foreigners;
213. Deputy Head of the Office for Foreigners;
214. Head of the Office for Veterans and Repressed Persons;
215. Deputy Head of the Office for Veterans and Repressed Persons.

APPENDIX 5

Whistleblowing Procedure

1. Each Employee has the right to anonymously report a potential or an actual breach of laws (in particular ML/TF), regulations, internal procedures or ethical standards ("**Breach Report**").
2. The Company protects the Whistleblower against revealing his identity and any repressive and/or discriminative actions or other kinds of unjust treatment.
3. Anonymity is provided by introduction of mechanism preventing verification of personal data of the Whistleblower. Therefore, the Breach Reports may be sent as follows:
    a. Placed in a locked designated letter box in the office, or;
    b. Sent by email to the Compliance officer or to the members of the board (if 9 below occurs).
4. All Breach Reports shall be submitted in designated electronic form, ensuring anonymity. The Breach Reports are sent to the Company's Compliance Officer.
5. Whistleblower must:
    a. act in a good faith;
    b. provide precisely all relevant information relating to the breach;
    c. respect confidentiality;
6. Whistleblowers are requested to provide following information:
    a. the date(s) of the event(s);
    b. the nature of the event(s);
    c. the name of the persons involved in the event(s);
    d. the names of possible witnesses to the event(s);
    e. evidence of the event(s), e.g. documents, emails, other.
7. Breach Reports not including sufficient information may not be investigated.
8. The Breach Reports shall be investigated by the Compliance Officer and Board of Directors or other persons designated by the Board.
9. In the event the Breach Report relates to Compliance Officer, the Breach Report shall be investigated by the Board or other authorized person.
10. In the event the Breach Report relates to a member of the Board, the Breach Report shall be investigated by the entire Board with the exception of the affected Member.
11. The preliminary investigation of the Breach Report must in principle be concluded within 1 month of receipt of the Breach Report.
12. If there are reasonable facts and/or circumstances resulting from the preliminary investigation proving that the reported Breach Report is sufficiently grounded, a full investigation shall be carried.
13. After closing of the investigation, the body conducting it shall specify subsequent actions, in particular their type and character, which should be taken.
14. In case where personal data of Whistleblower is known, he/she shall be informed about the results of closed investigation.
15. Persons investigating the Breach Report must never attempt to discover the identity of a Whistleblower who has chosen to act anonymously.
16. In case where the personal data of the Whistleblower is known, persons or bodies conducting investigation shall not pass such data to other persons and shall strive to limit to minimum a circle of persons who may have an access to data. Disclosure may be done but is not limited to a case where the Company is legally obliged to disclose the Whistleblower's identity; and/or the disclosure of such information is required if and when the Company decides to report to relevant authorities.

17. Whistleblower should comply with any reasonable requests to clarify any facts and/or circumstances, to provide (additional) information and to cooperate with an investigation.
18. A lack of additional requested information can be the reason for deciding not to conduct an investigation and/or to conclude that the Breach Report has no factual basis.
19. Neither the Whistleblower nor any other employee who provides information, who causes information to be provided or who otherwise assists in an investigation are allowed to discuss the details of the reported Breach Report or any related investigation with anyone except persons conducting investigation, unless specifically required by law.
20. After closing of investigation, possible personal data shall be anonymized in the Breach Report.
21. Company's Compliance Officer conducts initial and periodic trainings regarding this Procedure. Trainings may be conducted by distribution of an electronic presentation.
22. Company's Compliance Officer shall at least once a year inform the Board about the reported Breach Reports.
23. Company's Board of Directors shall at least once a year assess an adequacy and effectiveness of this process.