I. GENERAL PROVISIONS

1. Policy on prevention of money laundering and terrorist financing (hereinafter – **the Policy**) establishes the procedures of the company UAB Centurion Invest Lithuania (hereinafter – **the Company**) as obliged entity, for implementation and daily compliance of the legal requirements on prevention of money laundering and terrorist financing (hereinafter – **ML/TF**).
2. The Policy is prepared according to the Law on Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania No. VIII-275 (hereinafter – **the Law**), Order of the director of the Financial Crime Investigation Service Under the Ministry of Interior of the Republic of Lithuania "On instructions to deposit virtual currency wallet operators and virtual currency exchange operators to prevent money laundering and / or terrorist financing" (hereinafter – **the Order**), and other EU and national legal acts.
3. The main activity of the Company is the provision of virtual currency exchange and virtual currency deposit wallet services (hereinafter - **the Services**) and related services in the Republic of Lithuania. According to the Article 2 Paragraph 10 Points 10 an 11 of the Law, the Company as a virtual currency deposit wallet and exchange operator is obliged entity to provide services according to the Law in order to prevent ML/TF.
4. The Company assesses the risks of ML/TF using a risk-based approach and evaluates the following types of risks:
   4.1. risk related to the Customer's attributes;
   4.2. risk associated with the channel for the supply of a product, service, transaction, or service delivery
   4.3. risk related to the area (country and/or geographical).
5. The Policy is prepared considering that the Company does not provide financial services and cash services. All of the Company's services are provided electronically through a service platform (website) operated by the Company.
6. At least annually or in the case of significant events, the Company will carry out a risk assessment, monitor the adequacy of the measures set out in the Policy for the implementation of the ML/TF, where necessary, new or adequate preventive measures shall be amended or introduced.
7. This Policy must be followed by all employees of the Company. The obligations of the Company as defined in the Policy must be understood as the duties of all employees of the Company unless it is provided that certain duties of the Company must be performed by a specially designated employee of the Company.
8. The Company shall notify the Financial Crime Investigation Service (hereinafter – **the FCIS**) in writing of the appointment or change of the employee (hereinafter – **the AML Officer**) responsible for implementation of prevention of ML/TF measures in the Company no later than 7 business days after their appointment or change.
9. This policy shall be accepted and approved by the resolution of the CEO and the AML Officer.

II. RISK ASSESSMENT AND MANAGEMENT

9. The Company shall apply a risk-based approach when implementing measures to mitigate the risk of ML/TF.
10. The Company continually assesses and manages the ML/TF risks associated with the Company's business relationship or incidental transactions. The Company's risk assessment consists of:
    10.1. Risk assessment at the Company level, which covers all activities of the Company, helps identify areas in which the Company has to implement priority risk management measures commensurate with the risks and the business specificities of the Company, the scope of its activities;
    10.2. Risk assessment of relationships and transactions with customers and transaction validation, which includes identification, other KYC procedures and ongoing monitoring;
    10.3. Continuous monitoring of the level of risk arising from the ongoing monitoring of customer transactions, monetary operations and status to match the Company's customer profile and be not suspicious, ensuring that the information available to the Company is relevant, allowing an assessment of whether the level of risk has remained unchanged.
11. Comprehensive measures are applied by the Company to determine the risk of ML/TF both before and after establishing a business relationship with the customer, by analyzing the customer's behavior and monetary operations, transactions carried out and information provided (documents) by him/her.
12. Customers of the Company are divided into following three risk groups:
    12.1. Low-risk, customers who carry extremely low risk of ML/TF, including low risk to the Company's reputation. Low risk group customers include all those who fulfil one or more of the low-risk attributes listed in Annex 1 of this Policy.
    12.2. Medium-risk, customers rated as being at risk for some ML/TF by one or more attributes, but their status or operations carried out by them would not have the same impact on the Company's reputation as high-risk customers or activities thereof. Medium-risk group customers include all those who does not fall under low or high risk customer categories as indicated in Annex 1 of this Policy.
    12.3. High-risk, customers who has one or more of the attributes of increased risk of ML/TF and in respect of whom the Company has a reasonable suspicion that they may significantly adversely affect the Company's reputation. Higher risk group customers include all those who meet one or more of the high-risk attributes listed in Annex 1 of this Policy.
13. Customers are assigned to one of the identified risk groups when establishing business relationships. Subsequently, the risk profile of the customer may be changed in the light of the results of the monitoring of business relationship.
14. The customer risk assessment is built on the principle that higher risk is given a bigger risk score.
15. The establishment of the business relationship with high-risk customers must be approved by the AML Officer.
16. The customer risk assessment, both prior to establishing a business relationship and updating the customer's data, is performed by employees responsible for the customer's onboarding. Only after the customer's risk assessment is completed, a decision is made on establishing a business relationship.

17. When assessing the risk of the customers, the primary aim is to evaluate all information available about the customers.
18. During assessment of customer's risk and establishment of business relationship the Company shall collect dully filled-in and executed Company's customers and/or ultimate beneficial owner questionnaire(-s) in accordance to section V of this policy. The Company's customers and ultimate beneficial owner questionnaire are presented in annexes of this Policy, accordingly Annex 2 - Annex 4.

III. CUSTOMER'S TRANSACTIONS AND OPERATIONS MONITORING

19. After establishing a relationship with the customer, the customer's business relationships, including transaction and operations, are monitored on an ongoing basis- ongoing customer due diligence (ODD) is applied. This shall ensure that transactions and operations are consistent with the Company's information of the Customer, its business, risk profile and source of funds. The Company maintains real–time and retrospective monitoring of business relationships and operations.
20. Employees of the Company (incl. the CEO and the AML Officer) must monitor customer's transactions on an ongoing basis for any unusual operations or activities. Unusual features may be related to the size of the transaction, which is inconsistent with the customer's financial position or past known business, the customer's knowledge or experience, the unusual nature of the transaction as distinguished from other customer's methods of operation or similar usual business practices, the complex structure of the transaction as compared to similar transactions in a similar profile of the customer or the market. ODD also means that the Company periodic updates of customer's information.
21. In the event of any employee of the Company having any doubts about the legality, economic or legal validity of the customer's activities or of any particular operation or transaction, its non-consistence with customer's personal or business profile, sources of funds or financial capacity, the employee must immediately notify the AML Officer, who must then investigate further and determine decide on the necessity of reporting to the FCIS of the customer's activity or transaction.
22. When monitoring the customer's activities, transactions and operations, particular attention must be paid to:
    22.1. complex or unusually large transactions and any unusual transactional structures that have no apparent economic or visible legitimate purpose, and business relationships or operations with customers from third countries, where, in accordance with official information published by international intergovernmental organizations, measures to prevent ML/TF are insufficient or do not meet international standards.
    22.2. any threat of ML/TF that may arise from the use of the services provided or the transactions carried out in order to conceal the identity of the Customer or the beneficial owner, as well as in respect of any business relationship or transaction with the customer who has not been identified through direct presence and, where necessary, immediate measures are taken to prevent the use of money for ML/TF.
    22.3. whether the customer or a beneficial owner is included in the consolidated list of the United Nations of persons, groups and entities and bodies subject to EU financial sanctions.

22.4. whether the customer or the beneficial owner has no links with countries that are classified in the category of higher risk countries: they are subject to European Union sanctions or other restrictive measures, as well as to the countries identified by the Financial Action Task Force as high risk or non-cooperative countries.

23. The Company has ongoing control over its operations for possible violations of international sanctions. Depending on the nature of the Company's activities – provision of virtual currency services – the Company implements this obligation through a third-party monitoring tool.

24. The results and conclusions of unusual customer activities, transactions and operations investigations must be recorded in writing.

25. All communications to the FCIS are provided by the Company's CEO or the AML Officer who is assigned to perform this function.

26. In case the Company has established business relationship with the customer, determined as a high-risk customer, the Company applies enhanced ongoing customers due diligence (EODD). In addition to the measures applied for ODD, the Company shall monitor and analyze the following actions of high-risk customer:

26.1. Transaction types (e. g. series of high-value cryptocurrency transactions in a short period of time, instant withdraw of cryptocurrency deposits with no transaction activity);

26.2. Transaction patterns (e. g. frequent transfers of large amounts of crypto within a set period of time, to the same account from more than one person);

26.3. Anonymity (e. g. multiple cryptocurrency wallets controlled from the same IP address, IP associated with suspicious sources);

26.4. Senders and recipients (e. g. elderly or financially vulnerable customers engaging in high-volume cryptocurrency transactions);

26.5. Source of funds (e. g. transactions involving cryptocurrency accounts with known links to illegal activities, such as fraud, extortion, etc.).

27. If the employee (incl. the CEO and the AML Officer) becomes aware or otherwise suspects that a transaction, operation, or customer activity is suspicious, or for any other reason listed in this Policy would be reported to FCIS, he/she will promptly record it, re-examine, carry out further examination of the information available in order to assess whether there is a basis for providing such information to the FCIS and, where available, submit the information in the format, procedures and timelines set by the FCIS.

28. All employees of the Company, without exception, must be prohibited from informing the customer or any other person that information about the customer's operations or transactions, or any other information, has been provided to the FCIS or other supervisory authority.

29. The Company or its employees are not liable to the customer for failure to perform their contractual obligations or for damage if this occurs as a result of suspending an operation or transaction and reporting the allegations to the FCIS or because of failure by the customer to provide data to confirm his identity, or providing incomplete or incorrect information, or if customer or his representative avoids providing the information necessary to identify him/her.

30. No liability must be imposed on Company's CEO, the AML Officer or other employees who, in good faith, report information on suspected ML/TF or suspicious operations or

transactions to the FCIS. Likewise, they may not be subject to any disciplinary action by the Company.

31. The Company must notify the FCIS immediately, no later than within 1 (one) business day after the occurrence of such information or suspicion, if the Company is aware or suspects that assets of any value are directly or indirectly derived from a criminal offence or by participating in a criminal offence.
32. Where it is determined that the customer carries out a suspicious operation or transaction, regardless of the amount of the operation or transaction, it is mandatory to suspend the operation or transaction (unless due to the nature of the operation or transaction, the manner in which it is performed or other circumstances it is objectively impossible) and no later than 3 business hours from the time of the transaction or the suspension of the monetary operation to report this operation or transaction to the FCIS. If, due to the nature of the operation or transaction, the manner in which they are performed, or other circumstances, the operation or transaction has not been suspended, the FCIS must be notified no later than 3 business hours after such operation or transaction is identified. Immediate reporting is also required when the Company employees receive information that the Customer intends or will attempt to execute a suspicious operation or transaction.
33. The Company is required to unilaterally suspend a suspicious operations/transaction and upon receipt of a written order from the FCIS must suspend any suspicious operation or transaction performed by the customer for a period of up to 10 business days from the time or circumstances specified in the order. During this period, the Company's suspended transaction/operation may be renewed only with the permission of the FCIS.
34. If the Company is not obligated to execute the temporary restriction of the ownership rights within 10 business days after the notification or FCIS order has been received, the operation or transaction shall be resumed.
35. Notification of suspicious operations or suspicious transactions to the FCIS must be submitted by logging in to the FCIS information system and filling in the approved electronic form for the provision of information on suspicious operations or suspicious transactions.
36. Only in exceptional cases, should the Company not be able to access the FCIS information system and complete the information submission form, or would not be able to do so for other technical reasons, it may also, in emergency cases, submit the information to the FCIS by phone, fax or email.
37. The suspicious transaction report form must include:

    37.1. identity information of the customer, his representative (for natural persons – full name, date of birth, personal code; for legal entities – name, legal form of legal entity, registered address, legal code, if any).

    37.2. to what kind of criteria approved by the FCIS, to recognize that the operation or transaction is considered to be suspicious, the operation or transaction is in conformity.

    37.3. method for performing a suspicious operation or suspicious transaction.

    37.4. the date of the suspicious operation or suspicious transaction, a description of the property to which the transaction relates and its value.

    37.5. Deposit wallet management methods.

    37.6. contact information of the customer, his representative (phone numbers, e-mail addresses, contact persons).

37.7. A beneficiary in whose favor a suspicious operation or suspicious transaction is performed (for natural persons – full name, date of birth, personal code; for legal entities – name, legal form of legal entity, registered address, legal code, if any).

37.8. date and time of suspension of the suspicious operation or suspicious transaction.

37.9. if the suspicious operation or transaction has not been stopped, – the reasons for not stopping it.

37.10. other information that the Company considers relevant.

38. The Company will report to the FCIS the customer identifying data and information on executed virtual currency exchange operations or transactions in the virtual currency where the value of such monetary operation or transaction equals or exceeds EUR 15 000 in Fiat currency or virtual currency, regardless of whether the transaction is made in one or several related monetary transactions.

38.1. Multiple related transactions mean multiple virtual currency exchange operations or transactions in virtual currency during the day, where the total amount of operations and transactions equals or exceeds EUR 15 000 or the equivalent in fiat currency or virtual currency.

38.2. Notification of operations or transactions of EUR 15 000 or more must be submitted to the FCIS without delay and no later than 7 business days after the date of the execution of the monetary operation or transaction.

IV. IMPLEMENTATION OF SANCTIONS

41. The AML Officer is an employee appointed by the Company who arranges the implementation of financial sanctions, is responsible for suspending the disposal of the deposit wallets, regular updating of the list of entities subject to financial sanctions or the selection of eligible third party suppliers to provide consolidated updates of international lists of financial sanctions and quality control of their services, reporting to FCIS and other authorities responsible for overseeing the implementation of international sanctions.

42. The Company must:

42.1. implement financial sanctions.

42.2. Check in the consolidated databases used by the Company, and in their absence or if they are inoperative, in direct sources, whether the Company's customer and its beneficial owner are not included in the list of entities and their groups, which are subject to United Nations Security Council resolutions against terrorism, a consolidated list of the European Union's financial sanctions, as well as the lists of financial sanctions issued by the United States Treasury Department's Office of Foreign Control and/or the Republic of Lithuania.

42.3. pay particular attention to customers from countries on the lists of non-cooperating states and territories drawn up by the FATF and the European Commission, and operations or transactions carried out on their own or on their behalf.

42.4. restrict the right of customers included in the abovementioned international financial sanctions lists to operate, use and dispose of the virtual currency and the Fiat currency held in the Company, subject to the implementation exemptions provided for in international organizations decisions and/or European Union legislation.

42.5. immediately terminate or suspend the obligations incurred prior to the imposition of the international financial sanctions in the Republic of Lithuania for the period of the implementation of the international financial sanctions.

42.6. to terminate immediately – unilaterally or by agreement of the parties – transactions concluded prior to the imposition of financial sanctions in the Republic of Lithuania, or to suspend their execution for the period of implementation of financial sanctions.

42.7. inform the FCIS of the suspension of the accounts of the customers subject to financial sanctions.

42.8. provide information on the implementation of financial sanctions and all data necessary for supervision to the FCIS.

43. Company employees and customers are prohibited:

43.1. to carry out actions which are prohibited by international sanctions implemented in the Republic of Lithuania.

43.2. to enter into transactions which would be contrary to international sanctions implemented in the Republic of Lithuania.

43.3. to assume new obligations, the fulfilment whereof would be contrary to international sanctions implemented in the Republic of Lithuania.

V. CUSTOMER AND BENEFICIAL OWNER IDENTIFICATION

44. The Company's employees whose functions include performing prevention of ML/TF (hereinafter – **the Responsible employees**) are responsible for the identification of the customer, its representative and the beneficial owner, collection and initial verification of customer's, it's representative and beneficial owner data and documents.

45. The Company shall take steps to identify and verify the identity of the customer, its representative and the beneficial owner in the following cases:

45.1. Before starting business relationship.

45.2. Before performing occasional virtual currency exchange operations or occasional transactions in virtual currency equal to or exceeding EUR 700 or the equivalent in foreign or virtual currency, or by making an occasional deposit or withdrawal of virtual currency in the amount of or exceeding EUR 700 or the equivalent in a foreign or virtual currency, whether the transaction is concluded in one or more related transactions (the value of the virtual currency is determined at the time of the monetary transaction or transaction), unless the identity of the customer and the beneficial owner has already been established.

45.3. When there are doubts about the accuracy or authenticity of previously obtained customer and beneficial owner identities.

45.4. In any other case where there is a suspicion that ML/TF activities are, have been or will be carried out by the customer.

46. The Company's Responsible employees shall be responsible for reviewing the quality of the customer's file, verifying the data in independent reliable sources available to the Company (lists of politically exposed persons, international sanctions, etc.). These responsible employees shall also perform risk assessment and assignment of the customer to the risk category and other compliance procedures as provided in the Policy.

47. After gathering all the necessary information about the customer (dully filled-in and executed customer questionnaires), the Responsible employees first identifies the customer's risk group.
48. Upon making a decision to establish a business relationship with the customer, the Responsible employees, while providing the services to the customer, shall continue to monitor the customer on a regular basis.
49. Customer and beneficial owner has to provide the following documents and information for identification purposes:
    49.1. Passport or ID copy if customer, it's representative, beneficial owner is natural person.
    49.2. Utility bill indicating residence address of natural person.
    49.3. Apostilled or legalized commercial excerpt of the company if customer is legal entity (translated to English language).
    49.4. Apostilled or legalized Articles of Association of the company if customer is legal entity (translated to English language).
50. The Company only considers provided documentation form the customer suitable if scanned copies and/or good quality photos are provided to the Company.
51. In case the Responsible employee determines customer as a low-risk customer, the Company might does not apply rules indicated in point 49 of this Policy. The Company then:
    51.1. collects correctly filled-in and dully filled-in and executed customers questionnaires.
    51.2. ensures that the first payment of the customer would be carried out through an account with a credit institution, registered in a Member State of the European Union.
52. If the Responsible employee determines customers category as a high-risk, in addition to the documents listed in point 49 of this Policy, the Company shall:
    52.1. obtain additional information on the customer and on the beneficial owner;
    52.2. obtain additional information on the intended nature of the business relationship;
    52.3. obtain information on the source of funds and source of wealth of the customer and of the beneficial owner;
    52.4. obtain information on the reasons for the intended or performed transactions;
    52.5. obtaining the approval upon point 15 of this Policy;
    52.6. conduct EODD of the ongoing business relationship with these by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination;
    52.7. ensures that the first payment of the customer would be carried out through an account with a credit institution, registered in a Member State of the European Union.
53. It is forbidden to enter into transactions, to establish or continue business relationships, provide Services when customer identification is not possible in accordance with this Policy:
    53.1. if the customer does not provide data proving his identity.
    53.2. if the customer does not provide all data or data is incorrect.
    53.3. if the customer or his representative avoids providing the information necessary for his identification or avoids providing the information necessary to identify the beneficial owner, or the data provided is not sufficient.

54. If the customer avoids or refuses to provide additional information to the Company at its request and within the time limits, the Company shall take measures to mitigate the ML/TF risk in accordance with this Policy. The Company may also refuse to execute transactions or operations, suspend transactions or terminate business relationship with the customer. Upon termination of the business relationship, the Responsible employees must report such customer and other related information into the registration journal of customers with whom transactions or business relationships are terminated (Annex 5) in accordance with the procedure set forth in this Policy.
55. If proper identification, verification, or follow-up is not possible, Responsible employees of the Company who notices such a case must immediately notify the Company's AML Officer. The AML Officer shall decide on the advisability of reporting a suspicious operation or transaction report to the FCIS.
56. The customer and/or it's representative shall perform identity verification remotely via tools presented by the Company.
57. The documents, data or information submitted to the Company during the identification of the customer and the beneficial owner must remain true, accurate and up-to-date throughout the business relationship with the Company.
58. The data of customers, both existing and new, is updated as the circumstances surrounding the customer change, as new circumstances become evident, and periodically, depending on the customer's level of risk.
59. High-risk customer data must be updated at least once a year, medium-risk customer data is updated at least every 2 years, low-risk customer data is updated upon learning of any changes, but at least every 3 years.
60. If the customer has initiated updates in his account information, the changes must be evaluated, and risk should be reassessed accordingly.
61. If the changes in the customer's information resulted in a change of the customer's risk level, the date from which the customer's data must be updated is renewed according to their risk level.
62. If the customer did not update his/her data when required according to his/her risk level during the period of 3 months, services provided by the Company to the customer will be limited.
63. Updating of the data means that it is obligatory to check that the Company has up-to-date information about the customer, its representatives and beneficial owners. It is necessary to ensure that the transactions and/or operations executed by the customer so far comply with the information available to the Company on the customer, its activities and the source of funds.
64. During the review, it is always mandatory for customers to be screened for being included in the sanctions lists, changes in their status of politically exposed persons or existence of any negative information. If the functionality of the systems used by the Company allows, such verification must not be periodic, but is performed on a continuous basis through consolidated databases, whereby once entered, the customer's information is constantly verified and any changes in customer status are reported to the Company's CEO who periodically reviews system alerts for potential new results related to changes in the customer status and takes appropriate action.

65. Evidence of the review is stored in the customer's electronic file in the Company's database.

VI. KYC AND CUSTOMER DUE DILIGENCE

66. Customer due diligence (CDD) is a key responsibility of the Company in the implementation of the prevention of ML/TF and includes:
    66.1. Customer identification and verification based on provided documents, data and information obtained from an independent and reliable source.
    66.2. Identification of the beneficial owner and taking reasonable steps to verify that the named person is in fact the final beneficial owner and to verify his identity.
67. The data provided by the customer must be verified on the basis of documents, data or information obtained from a reliable and independent source.
68. The information must be verified by various means and sources available, including:
    68.1. checking the consistency of the information received (whether there are illogical or unexplained facts, inconsistencies).
    68.2. comparing the information provided by the customer with the content of official documents provided by the customer or received at the initiative of the Company, information contained in public registers.
    68.3. using targeted web search: for example, by typing in the customer's name and certain keywords, depending on the search context, using information available on social networks to identify the customer's relations, etc.
    68.4. using other reliable sources depending on the information to be verified.

VII. STORAGE OF INFORMATION

69. The Company shall maintain the following journals and database:
    69.1. Database/ journal for registration of customers with whom transactions or business relationships have been terminated in the cases provided for in the Policy or in other circumstances related to the prevention of ML/TF (Annex 5).
    69.2. Database/journal of virtual currency exchange operations or transactions in virtual currency amounting to or above EUR 15 000 or equivalent in Fiat currency or virtual currency (Annex 6).
    69.3. Database/journal of reports submitted to FCIS on suspicious operations and transactions (Annex 7).
70. The information in the listed registration databases shall be maintained and stored in the Company's information systems. Data may be entered in the databases no later than within 3 business days after the date of the transaction or suspension of transaction/termination of a business relationship, either manually or automatically.
71. Copies of the customer's identity documents, beneficial owner's identity data, other data received during the customer's identification, documentation shall be retained for 8 years from the date of termination of transactions or business relationships with the customer.
72. Business correspondence with the customer must be stored for 5 years from the end of transactions or business relationship with the customer in paper or electronic form.

73. Documents or information supporting operation or transaction or other legal instruments relating to the performance of operations or transactions must be stored for 8 years from the date of operation or transaction.
74. Documents analyzing the results of the transaction investigation are stored in electronic database for 5 years.
75. Retention periods may be further extended additionally for a period not exceeding 2 years, upon motivated instruction of the competent authority.

VIII. TRAINING OF THE COMPANY'S EMPLOYEES

76. All employees of the Company shall be introduced to the Policy upon their appointment by their signature. The CEO of the Company, must ensure that all newly recruited employees are made aware of this Policy in writing and receive training, depending on the functions performed by the employee.
77. The Company must review and, where necessary, update its internal control procedures:
    77.1. strengthen the applicable internal control procedures upon receipt of an order from the FCIS.
    77.2. upon significant events or changes in the Company's management and operations.
    77.3. periodic monitoring of the implementation and adequacy of internal control procedures.
78. The CEO of the Company must ensure that the relevant employees of the Company are aware of the legal acts and requirements applicable to them and the provisions of this implementing Policy. These measures shall include participation of their relevant employees in special ongoing training programs to help them recognize the actions which may be related to ML/TF and to instruct them as to how to proceed in such cases.
79. Responsible employees must continually upgrade their skills, following the Republic of Lithuania, European Union legislation updates, recommendations of FATF and other organizations, to seek to participate in the training on ML/TF prevention and enforcement of international sanctions (courses, seminars, internships, etc.).
80. The CEO of the Company also identifies the need for internal training of the Company's employees. Any other member of the compliance department may also indicate such need.
81. The CEO of the Company must ensure that Company's employees are informed in a timely manner of material events occurring inside or outside the Company, incidents affecting the effectiveness of prevention of ML/TF or sanctions.

IX. FINAL PROVISIONS

82. The implementation of measures for prevention of ML/TF is organized by the AML Officer in liaison with the FCIS.
83. The CEO of the Company must ensure that the AML Officer have access to all information necessary to perform their functions, including information relating to the identity of the customer and the beneficial owner customer's business relationship, cash operations and transactions, and other information.
84. This Policy is approved by the CEO and the AML Officer of the Company. This Policy and appendices to the Policy shall take effect from the date of its approval unless otherwise

specified. The Policy may be withdrawn, amended and/or supplemented only by a decision of the CEO and the AML Officer of the Company and shall enter into force on the day following the date of adoption of such amendments and/or additions. All employees of the Company are familiarized with the changes immediately.