25.05.2022

FOR INTERNAL USE ONLY

AML/KYC AND INTERNATIONAL FINANCIAL SANCTIONS PROCEDURES

INTERNAL CONTROL RULES OF AML ACT IMPLEMENTATION

1. DEFINITIONS AND ABBREVIATIONS

1.1. **Company** – Bizonex LLC, identification number: 414766984.

1.2. **Customer** – an individual or legal entity to whom the Company provides a service.

1.3. **Money laundering** is the concealment or disguise of the true nature, source, location, disposition, transfer, ownership or other rights with respect to property derived from criminal activity or property derived therefrom. Modification, transfer, acquisition, possession or use for the purpose of concealing or concealing the illicit origin of property or of assisting a person who has participated in a criminal activity in order to avoid the legal consequences of his or her actions. Money laundering also occurs when the criminal activity that resulted in the acquisition of the property used for money laundering took place in the territory of another state.

1.4. **Terrorist financing** means the allocation or raising of funds within the meaning of the Penal Code for the planning or commission of acts which constitute terrorism or for the financing of terrorist organizations, or with the knowledge that such funds are being used for such purposes.

1.5. **An international sanction** is a non-armed measure decided by the European Union, the United Nations, another international organization or the Government of the Republic Georgia to achieve or maintain peace, prevent conflict and strengthen international security, and to support and strengthen democracy, the rule of law, human rights and international law.

1.6. **Politically Exposed Person (PEP)** - is a natural person who performs or performed important functions of public authority, including the head of state, head of government, minister and deputy or assistant minister, member of parliament or similar legislative body, member of party governing body, member of Supreme Court, member of the board of directors and administrative or supervisory body of a state-owned enterprise, head of an international organization, deputy head and member of the management body or equivalent.

1.7. **Local PEP** - is a natural person specified in clause 1.6. who performs or performed important functions of public authority in Georgia.

1.8. **Family member of a PEP** - is a natural person considered to be equivalent to the person's spouse, a person's child and a person considered to be equivalent to the child's spouse and a person's parent.

1.9. **Close associate of a PEP** - means a natural person who is known to be the beneficial owner or joint owner of a legal person or entity with a national or local national or has a close business relationship with a national or a local national, and a natural person who is the sole beneficial owner

of a legal person or entity known to be effectively established for the benefit of a national or local national.

1.10. **AML Act** - Law of Georgia on Facilitating the Suppression of Money Laundering and Terrorism Financing .

2. GENERAL PROVISIONS

2.1. This guide has been prepared on the basis of the AML Act and the International Sanctions Act and is intended for internal use.

2.2. This Guide sets out internal security measures to comply with the requirements of due diligence in the prevention of money laundering and terrorism and international sanctions, and to detect suspicious and unusual transactions.

2.3. The employees of the Company must be familiar with and strictly follow the requirements of the AML Act, international sanctions, money laundering and terrorist financing suspicion transaction identification instructions, other instructions for complying with the AML Act and this guide.

2.4. The employees of the Company must independently get acquainted with the amendments to laws and other legislation.

2.5. The management board of a Company is obliged to introduce these instructions to all employees.

2.6. The employees of the Company are required to confirm the reading of these instructions.

2.7. The employees of a Company are personally responsible for compliance with the requirements of the AML Act pursuant to the procedure provided by law.

3. CUSTOMER RELATIONSHIP AND IDENTIFICATION

3.1. The employees of a Company shall apply the following rules of procedure each time before entering into a business relationship with a Customer.

3.2. The Company does not establish a customer relationship with the individual's authorized representative.

3.3. An individual customer is identified as follows:

3.3.1. The customer is identified on the basis of an identity document, a copy of the personal data and photo page of which is stored in the Company's customer base. Conducted the identification of the following documents: resident of Georgia – Georgian passport, identity card, alien's passport, residence card or a driving license; third country resident – travel document (passport).

3.3.2. The following data shall be recorded regarding an individual:

3.3.2.1. Name and surname.

3.3.2.2. Identity number, date and place of birth.

3.3.2.3. The name, number, date of issue and name of the issuing authority of the document used to identify and verify the person.

3.3.2.4. Residential address.

3.3.2.5. Means of communication: e-mail address and telephone number.

3.3.2.6. Whether the person performs or has performed functions as PEP.

3.3.2.7. Whether he/she is a PEP's close associate or a member of a family.

3.3.3. The following documents are required for customer identification:

3.3.3.1. Identity document. In the case of an Georgian resident, a Georgian citizen's passport, ID card, alien's passport, residence permit card, driving license issued in Georgia. In the case of a third-country resident, a travel document, or passport.

3.3.3.2. Document confirming the address of residence. Such document may be a utility bill, bank statement or other similar document that indicates the address and is not older than 3 months.

3.4. A legal entity customer is identified as follows:

3.4.1. The customer is identified on the basis of extract from Commercial Register, which is not older than 3 months, certified and, if applicable, apostilled.

3.4.2. The following data shall be recorded regarding a legal entity:

3.4.2.1. Name.

3.4.2.2. Registration number and date of registration.

3.4.2.3. Registered address and operational address details.

3.4.2.4. Representative's, shareholder's and beneficial owner's details.

3.4.2.5. Means of communication: e-mail address and telephone number.

3.4.2.6. For each individual in the legal entity (eg Director, Shareholder, Beneficial owner) details and documents as indicated in clause 3.3.

4. RISK ASSESSMENT AND DETERMINATION OF THE LEVEL OF MAINTENANCE MEASURES TO BE IMPLEMENTED

4.1. Establishing a business relationship with a Customer, Company needs to assess the degree of risk of money laundering and terrorist financing and, accordingly, to select and implement appropriate due diligence measures.

4.2. The following categories must be taken into account when assessing the level of risk of money laundering and terrorist financing:

4.2.1. Geographical risk.

4.2.2. Customer risk.

4.2.3. Transaction risk.

4.3. A geographical risk is considered high when the customer or transaction has a known relationship with the following countries or territories:

4.3.1. Countries and territories subject to a UN or European Union sanction, embargo or other similar measure.

4.3.2. Countries without adequate measures to prevent money laundering and terrorist financing.

4.3.3. Countries that, according to reliable data, are involved in supporting terrorism or have a high level of corruption.

4.3.4. Information on high-risk countries can be found at http://www.fatf-gafi.org/countries/#high-risk.

4.4. The customer's risk is considered high if the customer:

4.4.1. Is a PEP, a family member or a close associate of a PEP. The employees of a Company are required to establish whether or not they are the specified person before establishing a business relationship with the Customer and concluding the transaction.

4.4.2. It is included in the UN or European Union list of persons subject to international financial sanctions. Company's employees have a duty to monitor the information and before establishing a business relationship with the customer's data check.

4.4.3. There is a natural person who is previously suspected of being involved in money laundering or terrorist financing.

4.4.4. Is a natural person whose legal and/or actual address is in the high-risk jurisdiction;

4.4.5. carried out a transaction through the financial institution, which is located in the high-risk jurisdiction.

4.5. The risk associated with a transaction is considered high if:

4.5.1. A person who is not a party to the transaction shall pay for the transaction.

4.5.2. A transaction is requested, one of the purposes of which is to conceal the actual participants in the transaction.

4.5.3. A transaction is requested that does not have a clear reasonable commercial, economic, tax or legal purpose.

4.5.4. Virtual currencies are always received from different addresses or money received from different accounts.

4.5.5. Amounts of virtual currency or money are not usual for the customer.

4.5.6. Each time the customer receives different virtual currencies.

4.6. The risk of money laundering or terrorist financing is considered high if, for any reason, there is a suspicion that the customer or the transaction made by the customer may be related to money laundering or terrorist financing.

4.7. The Company does not offer a service or establish a customer relationship with:

4.7.1. The residents of high risked countries (http://www.fatf-gafi.org/countries/#high-risk).

4.7.2. Persons from the list of international financial sanctions.

4.7.3. PEP's and their family members or a close associate.

4.7.4. Persons, who is previously suspected of being involved in money laundering or terrorist financing.

4.8. Within not listed in clause 4.7. risks, to the customer must be applied enhanced due diligence measures.

5. IT RISKS AND THEIR MANAGEMENT

5.1. The risks associated with the technologies used are:

5.1.1. Information leak;

5.1.2. Providing of false information;

5.1.3. Malware and cyber-attack;

5.1.4. Risks related to the operation of the information system.

5.2. In order to mitigate the risks of information leakage, the employees of Company are required to:

5.2.1. Use only the private limited companies' internal servers;

5.2.2. Use software approved and installed by the Management Board of the Company, which is constantly updated;

5.2.3. Use Company hardware. The use of your own hardware, including external media , is strictly prohibited.

5.3. To reduce the risk of providing false information:

5.3.1. To confirm the data with the Customer, Company must perform the conversation with a personal meeting or during a videoconference.

5.3.2. In case of submitting false information of suspicion is required to ask the corroborating documents from the Customer.

5.4. To mitigate the risks of malware and cyber-attacks:

5.4.1. The system is constantly monitored to identify suspicious and unusual transactions.

5.4.2. System security tests are performed on an ongoing basis.

5.4.3. Software that is constantly updated is used to detect malware and fight viruses.

5.5. To mitigate the risks related to the operation of the information system:

5.5.1. A fail-safe network and server infrastructure is used.

5.5.2. A separate master server and a backup server are used. For security purposes, the master server and the backup server are located in different locations.

5.5.3. The information system of the Company is certified with the PCI / DSS standard.

5.6. According to the need, but at least once a year, information security trainings are organized for the employees of the Company.

6. APPLICATION OF DUE DILIGENCE MEASURES

6.1. Particular attention must be paid to the activities of the person or Customer involved in the transaction and to circumstances that indicate or are likely to involve money laundering or terrorist financing, including complex, high-value and unusual transactions that do not have a reasonable economic purpose.

6.2. The applicable due diligence measures are:

6.2.1. Identification of the customer or person participating in the transaction on the basis of documents and data submitted by him or her, and via video conference.

6.2.2. Identification of the beneficial owner.

6.2.3. Obtaining information about the Customer's business relationship and the purpose and nature of the transaction.

6.2.4. Continuous monitoring of the customer's business relationship, including monitoring of transactions performed during the business relationship, regular verification of identification data, updating of relevant documents, data and information and, if necessary, identification of the source and origin of funds used in the transaction.

6.3. When applying due diligence, the facts to be established are generally determined on the basis of the original documents submitted by the customer. If the original document cannot be obtained, notarized or officially certified documents, including documents certified by a lawyer, may be used. If this is not practicable given the degree of risk, a copy of the original document must be stamped and / or signed by the issuer and may be transmitted electronically (in a resubmitted written form). The copy may not be relied upon if there is any doubt as to its conformity with the original.

6.4. The application may rely on information that is written in the format, resulting in the commercial register a credit institution or a foreign credit institution branches or credit institution which is registered or in a third country where there are equal AML/KYC requirements.

6.5. The aforementioned due diligence measures must be applied before a business relationship or transaction is established.

6.6. The identity of the Customer may be established and the information provided verified during the establishment of the business relationship or the conclusion of the transaction, if this is necessary in order not to interrupt the normal course of business and if the risk of money laundering or terrorist financing is low. In such a case, the due diligence measures must be terminated as soon as possible after the first contact has been established and before any binding action is taken.

6.7. Where applicable, the person or Customer involved in a transaction or professional activity shall be required to certify with his or her signature the accuracy of the information and documents submitted for the application of due diligence measures.

7. APPLICATION OF ENHANCED DUE DILIGENCE MEASURES

7.1. Due diligence measures must be implemented in enhanced manner if:

7.1.1. The identity of the person or customer involved in the transaction is established and the information provided without being present at the same place as the inspected person or customer.

7.1.2. Identification or verification arises in doubt or arises suspicion in authenticity of the document’s or impossible to identify beneficial owner(s).

7.1.3. The nature of the situation involves a high risk of money laundering or terrorist financing.

7.2. Company's employee must apply at least one of the following enhanced due diligence measures:

7.2.1. Identify and verify the information provided by additional documents, data or information derived from a reliable and independent source or in the commercial register a credit institution or a foreign credit institution branches or credit institution which is registered in or having a place of business in the country where are equal AML/KYC requirements and if the identity of the person is established in that credit institution while in the same place as the person.

7.2.2. EDD implementation of the authenticity of the documents and verify the accuracy of the information contained therein, including their notarized or official confirmation of the correctness of the data collection, or a document issued by the credit institution as named in clause 7.2.1.

7.2.3. Perform first payment through the account, which is open to a person's name, who is involved in the transaction, with a credit institution, which is registered or acts in the country where are equal AML/KYC requirements.

8. IDENTIFICATION OF A PEP

8.1. When establishing a business relationship (upon concluding a customer agreement), the Customer fills in a form in which he or she enters the main mandatory data necessary for identification and verification and required by law.

8.2. Among other information, the Customer must indicate whether he, his family member or close associate is a PEP.

8.3. If the Customer's family member or close associate is a PEP, the Customer must also indicate the data of this person.

8.4. Information of PEPs is checked by the Company' employees from public sources, for example at https://namescan.io/FreePEPCheck.aspx.

9. IDENTIFICATION OF A PERSON SUBJECT TO INTERNATIONAL SANCTIONS

9.1. When establishing a business relationship (upon concluding a customer agreement), the Customer fills in a form in which he or she enters the main mandatory data necessary for identification and verification and required by law.

9.2. According to the information provided by the Customer, the employee of the Company exercises control over the international sanctions applied to the Customer.

10. IDENTIFICATION OF MONEY LAUNDERING SUSPICIONS

10.1. This section sets out the circumstances that indicate the suspicion of money laundering, to which the employees of the Company must pay special attention.

10.2. Self-undercover. The signs of a shadow are:

10.2.1. The appearance and conduct of a person are not in accordance with the nature of the transaction performed by the person or his or her conduct raises doubts.

10.2.2. The person is unable to complete the documents or uses outside assistance for this purpose.

10.2.3. The person has a previous suspicion of an undercover agent.

10.3. The person cannot justify the necessity of the service.

10.4. The person is requesting unusually high limits.

10.5. An unusual cash transaction.

10.6. Individual large or periodic small exchanges of virtual currency, if such activity does not correspond to the person's economic activity or is unusual.

10.7. Money received for virtual currency is requested to be transferred to another person's or a bank account in another country.

10.8. The person does not provide data and / or explanations about the transaction.

10.9. A large number of virtual currencies are exchanged if they are not in the ordinary course of the person's business or are unusual.

10.10. The person cannot be identified or will try not to provide your information.

10.11. The person is trying to enter into a fictitious transaction.

10.12. When creating a long-term customer relationship, a person wants to settle only in cash.

10.13. There is a suspicion that a person is acting in the interests of someone else.

10.14. A person wishes to settle in cash in the amount of more than 10,000 euros.

10.15. The person repeatedly settles in cash in amounts exceeding 10,000 euros.

10.16. Payment is made through a bank established in the tax-free territory.

11. REFUSAL TO CONCLUDE A CONTRACT AND CONCLUDE A TRANSACTION

11.1. The Company does not enter into a contract and does not perform a transaction:

11.1.1. With a person under 18 years of age.

11.1.2. With the individual customer's authorized representative.

11.1.3. With a person who refuses to provide the information and documents referred to in clause 3 of these rules, or provides less information than required, or tries to conceal something.

11.1.4. With a person in suspicion of an ambush.

11.1.5. With a person, whose provided documents or the obtained by the Company information points, that there is a suspicion of money laundering or terrorist financing

11.1.6. With a person subject to international financial sanctions.

11.1.7. With a person who is PEP or his family member is PEP or he/she is a close associate of PEP.

11.1.8. With a person who is previously known to be suspected of being involved in money laundering or terrorist financing.

11.1.9. With a person resident of high-risk country (http://www.fatf-gafi.org/countries/#high-risk).

12. DATA COLLECTION, STORAGE AND PROTECTION

12.1. Upon entering into a transaction, an employee of a Company is required to register the following information:

12.1.1. Details of the person participating in the transaction, in accordance with clause 3 of these instructions.

12.1.2. Date or period of the transaction.

12.1.3. Description of the content of the transaction.

12.1.4. Information on refusing to establish a business relationship or enter into a transaction.

12.1.5. Information on the waiver of the establishment of a business relationship or the conclusion of a transaction at the initiative of the Customer.

12.1.6. Information on the termination of the business relationship, including the impossibility of applying due diligence measures.

12.1.7. Virtual currency in exchange for cash exchange service, currency amount, amount of money and exchange rate.

12.1.8. The exchange rate of the virtual currency against another virtual currency, the amount of the currency, the amount of the other currency and the exchange rate.

12.1.9. When opening a virtual currency account, its type, number and currency name.

12.2. The Company shall keep the following documents for at least five (5) years after the termination of the business relationship or the conclusion of the last transaction:

12.2.1. Information to identify and verify the data and documents.

12.2.2. Correspondence with the Customer.

12.2.3. Data collected during business relationship monitoring.

12.2.4. Data on suspicious and unusual transactions.

12.2.5. Transaction documents.

12.3. Employees of a Company are required to apply personal data protection rules when collecting and storing data and documents. The data collected may only be processed for the purpose of preventing money laundering and terrorist financing. Processing of data in a way that does not meet this purpose is strictly prohibited.

13. FIU NOTIFICATION

13.1. If a Company employee detected the action or circumstances which indicate money laundering or terrorist financing, or where it suspects or knows that it is a money laundering or terrorist financing, it shall immediately inform the company's MLRO.

13.2. It is prohibited to inform the customer about the transmission of information to MLRO.

13.3. The MLRO shall attach copies of the documents on which the transaction is based, as well as copies of the documents on the basis of which the person is identified, to the completed notification form. The notice may be accompanied by copies of other documents characterizing the nature of the transaction.

14. INTERNAL CONTROL AND STAFF TRAINING

14.1. Compliance with the requirements of AML Act, International Sanctions Act and legislation established on the basis thereof is monitored and controlled by the Management Board of the Company.

14.2. Risk assessment and customer identification are performed by the trained employees of the Company and controlled by the Management Board of the Company.

14.3. Customers activity and operations are checked by the trained employees of the Company and controlled by the Management Board of the Company.

14.4. The Management Board of the Company is responsible for training the employees of the Company in the field of money laundering and terrorist financing prevention and compliance with the requirements of international sanctions.

14.5. Employees are required to independently review amendments to laws and other legislation.

14.6. Trainings for the Company’s employees takes place as needed, but not less than once a year.

Annex 1

KYC QUESTIONNAIRE FOR INDIVIDUALS

I. DETAILS

1. Name and surname
2. Date and place of birth
3. Tax residency
4. Tax ID
5. Address
6. E-mail
7. Phone number
8. Is customer, customer's family member or close associate is politically exposed person. If yes, indicate name and position.

II. DOCUMENTS

1. Passport (for EU citizens passport or national ID)
2. Address confirmation (bank statement with address, utility bill)
3. Selfie photo with document from clause 1.

Annex 2

KYC QUESTIONNAIRE FOR LEGAL ENTITIES

I. LEGAL ENTITY DETAILS

1. Name
2. Registration number
3. Registration date
4. Tax residency
5. Tax ID
6. Legal address
7. Operating address
8. Phone number
9. E-mail
10. Website (if exists)
11. Description of business

II. LEGAL ENTITY DOCUMENTS

1. Certified and apostilled registration certificate including director's, shareholder's and beneficiary details.
2. Address confirmation (bank statement with address, utility bill).

III. DIRECTOR'S DETAILS

1. Name and surname
2. Date and place of birth
3. Tax residency
4. Tax ID
5. Address
6. E-mail
7. Phone number
8. Is director, director's family member or close associate is politically exposed person. If yes, indicate name and position

IV. DIRECTOR'S DOCUMENTS

1. Passport (for EU citizens passport or national ID)
2. Address confirmation (bank statement with address, utility bill)
3. Selfie photo with document from clause 1.

V. SHAREHOLDER'S DETAILS AND DOCUMENTS

1. If shareholder individual – details from section III. and documents from section IV.
2. If shareholder legal entity – details and documents from sections I.-VI.

VI. BENEFICIARY DETAILS AND DOCUMENTS

1. Details from section III. and documents from section IV.