**AML POLICY**

**H3 Limited Liability Company**

**1. GENERAL TERMS**

1.1. This AML Policy of **H3 Limited Liability Company**, ID # 412770265, with financial license # 0110/571 (hereinafter - Company, H3) is based on international standards of anti-money laundering legislation, including [Financial Action Task Force (FATF)](https://sanctionscanner.com/knowledge-base/financial-action-task-force-fatf-368%22%20%5Ct%20%22_blank) standards, and fully complies with the requirements of the Law of Georgia on facilitating the prevention of money laundering and the financing of terrorism # 5226-Iს dated 30/10/2019. This AML Policy is adopted as a local regulation of the company for the purposes of assuring the compliance with the due diligence requirements for the prevention of money laundering and terrorist financing, identification of unusual transactions and performance of the obligations set out in the International Sanctions Act.

1.2. For the purposes of this AML Policy, security measures are understood to mean the measures applied by H3 in its business activities in relation to::

1.2.1. identify the parties of a transaction or an operation;

1.2.2. achieve the necessary care;

1.2.3. avoid fraudulent dealing, errors or other abuse of H3;

1.2.4. assure adequate performance of obligations arising from relevant legislation.

1.3. The employees of H3 should know and strictly follow the requirements set out in the Money Laundering and Terrorist Financing Prevention Act, guidelines issued by the Financial Intelligence Unit on the characteristics of suspicious transactions, other guidelines on the performance of the requirements of the Money Laundering and Terrorist Financing Prevention Act regulating the work of H3, the International Sanctions Act and the current procedure.

1.4. The employees of H3 should also independently familiarize themselves with changes to other legal acts that are published on the homepage of the FATF (https://www.fatf-gafi.org)

1.5. The employees of H3 shall confirm that they have read this manual with their hand-written signature.

1.6. The employees of H3 are responsible for personally following the requirements set out in the Money Laundering and Terrorist Financing Prevention Act, The International Sanctions Act and other related normative acts in accordance with law.

**2. TERMS**

2.1. Money laundering means the concealment of the true nature, origin, location, manner of disposal, relocation or right of ownership of property acquired as a result of a criminal activity or property acquired instead of such property or the concealment of other rights related to such property; the conversion or transfer of property derived from criminal activity or property obtained instead of such property for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person’s actions. Money laundering is regarded as such also where a criminal activity which generated the property to be laundered was carried out in the territory of another country.

2.2. Terrorist financing means the provision and collection of funds for the financing and planning of an act of terrorism and commissioning thereof or for the financing of a terrorist organization or while being aware that such funds will be used for the aforementioned purpose.

2.3. Politically exposed person means a natural person who performs or has performed prominent public functions and also family members and close associates of such person. A person who has not performed prominent public function for at least one year prior to the transaction date nor their family members and close associates shall not be considered a politically exposed person. Public search facilities (www.google.com) shall be used for the identification of a politically exposed person.

Persons deemed to perform prominent public functions within the meaning of the current procedure are:

1) a head of State or head of government, minister, deputy minister or assistant minister;

2) a member of Parliament;

3) a justice of the supreme court, constitutional court and other such higher court the decisions of which can only be appealed in exceptional cases;

4) a member of the state audit office or board of central bank;

5) an ambassador, commissioner or active serviceman with a military rank in the higher-level officer category;

6) a member of a state-owned company`s management, supervisory or administrative body. This term includes the positions within the European Union and other international organizations.

Family member of a politically exposed person means their:

1) spouse;

2) person considered to be equivalent to a spouse according to the legislation of the state of residence of such person or a person who has shared the same household as that person for at least one year on the date of the making of the transaction concerned;

3) children and spouses or a person considered to be equivalent to a spouse within the meaning of clause 2;

4) parent.

Person known to be close associates of a politically exposed person means:

1) a natural person who is known to have close business relations or joint beneficial ownership of a legal person or legal arrangement with a politically exposed person;

2) a person who is the beneficial owner of a legal person or legal arrangement known to be set up in the interests of a politically exposed person.

2.4. International financial sanction means international sanction that fully or partially prevents a subject of international financial sanction from using and disposing of financial means or giving thereof to its possession.

2.5. Subject of international sanction means a natural or legal person, an agency, a civil law partnership or any other entity which is directly specified in the act on the imposition or implementation of international sanctions and with regard to whom the measures prescribed therein are taken.

2.6. The Money Laundering and Terrorist Financing Prevention Act regulates the activities of credit and financial institutions and other undertakings and institutions set out in the Money Laundering and Terrorist Financing Prevention Act, also the activities of the Financial Intelligence Unit for the prevention of money laundering and terrorist financing.

2.7. Compliance officer means an employee appointed by the decision of the management board of the company who shall act as a contact person of the Financial Intelligence Unit and assure the compliance of institutions with the measures for the prevention of money laundering and terrorist financing. The compliance officer appointed by the management board is: Alexander Liske.

2.8. Person in charge means a person appointed by the decision of the management board who shall act as a person in charge of the Financial Intelligence Unit and assures that the entity that appointed them would comply with the requirements of the INTERNATIONAL SANCTIONS ACT. The person in charge appointed by the management board is: Alexander Liske.

2.9. Customer means a person who uses one or multiple services provided by the institution.

2.10. Business relationship within the meaning of this procedure means the services of the company established in an agreement concluded with a customer.

2.11. Loyal customer is a customer with whom a contract has been concluded.

2.12. The Financial Intelligence Service for the purposes of this AML Policy is defined in accordance with the Law of Georgia on Assistance in the Prevention of Money Laundering and Terrorist Financing No. 5226-Iს dated 30/10/2019 as a government agency responsible at the national level for receiving and analyzing confidential information related to possible the fact of money laundering and/or terrorist financing, as well as for the transfer, if necessary, of this information to another competent authority. (https://matsne.gov.ge/ru/document/view/4690334?publication=2)

**3. RISK LEVELS**

3.1. Within the meaning of the current code of conduct, transactions shall be categorized as follows:

3.1.1. low-risk transactions of up to 15,000 euros for individuals and transactions of up to 100,000 euros for legal entities;

3.1.2. high-risk transactions from 15,001 euros and up for individuals and more than 100,001 euros for transactions made by legal entities.

3.2. Within the meaning of the current code of conduct, customers shall be categorized as follows:

3.2.1. low-risk customers;

3.2.2. high-risk customers.

3.3. A low-risk customer means:

3.3.1. a person who has or has had a customer relationship with H3 as a payment service provider;

3.3.2. A natural person who, when making transactions with the company, does not give rise to or has no associated financial claims and obligations, the value of which would exceed 15,000 euros.

3.3.3. A legal entity that, when making transactions with the company, does not give rise to or has no associated financial claims and obligations, the value of which would exceed 100,000 euros.

3.4. A high-risk customer means:

3.4.1. a politically exposed person, their family member or close associate;

3.4.2. a natural person with associated financial claims and obligations with a value of no less than 15,001 euros;

3.4.3. a ltgal entity with associated financial claims and obligations with a value of no less than 100,001 euros;

3.4.3. a person who has been previously punished pursuant to criminal procedure, according to the information available to H3.

3.5. Considering that the list of potential customers of H3 does not include customers subject to a simplified identification procedure, the specified procedure has not been provided.

3.6. Special attention should be paid to the activities and circumstances regarding a person who has a business relationship with or conducts a transaction or operation or is planning to establish a business relationship or conduct a transaction or operation with H3 that suggest that the person is subjected to international sanctions.

3.7. H3 employees should regularly check the websites of the US and EU governments, as well as monitor the sanctions imposed by the UN, since it is on these resources that changes or termination of financial sanctions are published, as well as measures established in a legal act imposing or applying international financial sanctions . This AML Policy establishes an obligation for H3 and its employees to strictly comply with all EU and US sanctions.

3.8. Upon entry into force, amendment, repeal or expiration of a legal act imposing or applying an international financial sanction, it should be checked whether the person who has a business relationship with or conducts a transaction or operation or is planning to establish a business relationship or conduct a transaction or operation with H3 is subjected to an international financial sanction to be established, amended or terminated.

3.9. If a legal act imposing or applying an international financial sanction is repealed, expires or is amended in a manner that the application of an international financial sanction to a subject of an international financial sanction is partially or fully terminated, the application of the measure should be stopped in the extent established in the legal act that amends the legal act imposing or applying the financial sanction.

**4. ENHANCED DUE DILIGENCE**

4.1. Enhanced due diligence measures are applied when:

4.1.1. upon identification of a person or verification of submitted data, there are doubts as to the truthfulness of the submitted data, authenticity of the documents or identification of the beneficial owner;

4.1.2. the person or a customer participating in a transaction made in economic or professional activities is a politically exposed person, their family member or close associate in a European Economic Area country or a third country;

4.1.3. the person participating in an official operation, the person using an official service or the customer is from a high-risk third country;

4.1.4. the nature of a situation carries a high risk for money laundering or terrorist financing.

4.2. While applying enhanced due diligence, an employee shall also consider the relevant guidelines concerning risk factors that have been established by European supervisory authorities.

4.3. In the abovementioned case, the employee shall apply at least one of the following due diligence measures:

4.3.1. identification of the customer and verification of the submitted information based on additional documents, information or data obtained from a reliable and independent source or from a credit institution or the branch of a foreign credit institution registered in the commercial register or a credit institution established or having its place of business in a contracting state of the European Economic Area or in a country that applies requirements equal to those of the Money Laundering and Terrorist Financing Prevention Act, and if the person has been identified in the credit institution by using face-to-face identification;

4.3.2. application of enhanced due diligence measures in order to verify authenticity of the documents and the truthfulness of the data included in such documents, among other things, requesting their notarial or official certification or verification of the authenticity of the data by the credit institution that issued the document;

4.3.3. the making of the first payment related to a transaction via an account that has been opened in the name of the person or customer participating in the transaction in a credit institution registered or having its place of business in a contracting state of the European Economic Area or in a country where requirements equal to those of the Money Laundering and Terrorist Financing Prevention Act.

4.4. If the person participating in an official operation, the person using an official service or the customer is from a high-risk third country, the following due diligence measures shall be applied:

4.4.1. gathering additional information about the customer and its beneficial owner;

4.4.2. gathering additional information on the planned substance of the business relationship;

4.4.3. gathering information on the origin of the funds and wealth of the customer and its beneficial owner;

4.4.4. gathering information on the underlying reasons of planned or executed transactions;

4.4.5. receiving permission from the senior management to establish or continue a business relationship;

4.4.6. improving the monitoring of a business relationship by increasing the number and frequency of the applied control measures and by choosing transaction indicators that are additionally verified.

4.5. While choosing the due diligence measures, the employee shall consider in addition to clause 4.3. the relevant guidelines concerning risk factors that have been established by European supervisory authorities.

4.6. It is not allowed to establish a business relationship or conduct a transaction, if:

4.6.1. a person wants to make a cash payment of no less than 15,000 euros or an equal amount in another currency, regardless of whether the financial obligation is performed in the transaction in a lump sum or by way of several linked payments, and they do not submit documents and data required for applying the due diligence measures;

4.6.2. The submitted documents or other data give the employee a reason to suspect money laundering or terrorist financing.

4.7. The employee shall immediately notify the compliance officer of their suspicions.

4.8. The employee has the right to refuse from making a transaction if a person, regardless of the respective request, does not submit documents that would prove the legal origin of the cash or other property that is the subject-matter of the transaction.

4.9. The long-term contract serving as the basis for the business relationship may be extraordinarily terminated if the person participating in a transaction made in economic or professional activities or the customer does not, regardless of the respective request, submit documents and relevant data or if the submitted documents and data do not eliminate the suspicions of the person in charge that the objective of the transaction or the business relationship might be money laundering or terrorist financing.

4.10. Information regarding the refusal to establish a business relationship or conduct a transaction and the circumstances of the termination of the business relationship and/or the suspicion of money laundering or terrorist financing shall be registered and stored pursuant to procedure provided by law.

4.11. Identification of risks relating to new and existing technologies, and services and products. Prior to offering a new banking service or product, new or non-traditional sales channels to customers or the implementation of new or emerging technologies, the management board of H3 assesses in collaboration with the compliance officer the associated risks of money laundering or terrorist financing. The risks associated with new and emerging technologies are customer anonymity and the risks of fraudulent activity by using the identities of another person.

4.12. During risk assessment both actual and potential risks are assessed and, if necessary, additional data collected regarding the risks and their mitigation.

4.13. After the assessment of risks and their effects, H3 shall determine the most suitable countermeasures for mitigating the specific risks and bringing them to a level acceptable for H3 and, if necessary, organizes the implementation of such countermeasures. The risks associated with anonymity and fraudulent conduct shall be avoided by the identification of persons, during which a person is requested to submit a copy of an identity document and confirm its authenticity. In addition, the person will be requested to prove their residence by submitting copies of service invoices that include both the address of their place of residence and its connection to the specific person. If the person does not prove the specified circumstances or H3 has suspicions about the authenticity of the submitted documents, H3 will refuse to provide services to the customer.

4.14. H3 shall assess whether the application of countermeasures would make it possible to lower the risks of money laundering and terrorist financing associated with new banking services or products, new or non-traditional sales channels or new or emerging technologies to a level where they would be in accordance with the risk appetite of H3.

4.15. New banking services or products, new or non-traditional sales channels may be offered to customers or new or emerging technologies introduced only if the associated risks of money laundering and terrorist financing are in accordance with the risk appetite of H3 or they can be lowered to an acceptable level with the implementation of countermeasures. At that, it is not allowed to conclude a contract or make a decision on opening an anonymous account.

**5. IDENTIFICATION OF PERSONS IN THE PROCESS OF CONDUCTING TRANSACTIONS AND ESTABLISHING CUSTOMER RELATIONSHIPS**

5.1. Identification of persons is a process carried out by an employee of H3, during which the personal name, personal identification code or registry code or, where none, the date of birth and the place of residence or seat and other information required by this procedure.

5.2. The employee of H3 shall apply the following procedural rules prior to each transaction made with the customer and prior to establishing a business relationship:

5.2.1. identifies the customer, the person participating in a transaction or their representative, verifies the authenticity of the submitted documents and data and documents in writing the following personal data regarding the person participating in a transaction:

given name and surname; – personal identification code or date of birth; – place of birth; – address of the place of residence; – profession or field of activity; – document title, number, the date of issue, and the name of the issuer;

5.2.2. makes a copy of the page of the identity document containing personal data and a photo;

5.2.3. identifies the purpose of the transaction and the intended nature of the business relationship.

5.3. An employee of H3 is not allowed to make a transaction or conclude a contract:

5.3.1. with a person who refuses to submit the aforementioned information, also with a person who the employee suspects to be acting under covert identity;

5.3.2. if a customer does not submit the requested documents and relevant data or, if on the basis of the submitted documents there are grounds to suspect money laundering or terrorist financing.

5.3.3. Any incident specified in this part must be immediately forwarded to the compliance officer of the Financial Intelligence Unit while documenting as much customer identification data as possible.

5.4. The following valid documents may be used for the identification of a natural person:

5.4.1. According to the legislation of the European Union, the United States of America, Georgia, identity documents of an individual can be

5.4.1.1. identity card; – an passport; – a diplomatic passport; – a seafarer’s discharge book; – an alien’s passport; – a temporary travel document; – a travel document for a refugee; – a certificate of record of service on ships; – a certificate of return; – a permit of return

5.4.2. a valid travel document issued by a foreign state.

5.5. The following valid documents may be used for the identification of a legal person:

the name or business name of the legal person; – registered office; – the registry code or registration number; – date of issue of the document, and the name of the issuer; – the name and personal identification code of the representative of the legal person, date of issue of the identity document and the name of the issuer, presence and grounds for the right of representation.

5.6. The following valid documents may be used for the identification of a legal person:

5.6.1. the registry card of the relevant register that has been issued by a competent authority or body not earlier than six months prior to its submission.

5.6.2. the extract from a relevant register of a foreign country or the true copy of the registration certificate or an equal document that has been issued by a competent authority or body not earlier than six months prior to its submission (applied to a foreign legal person).

5.7. An employee of H3 shall additionally document the following on the legal person:

5.7.1. the names of the director, members of the management board or other body replacing the management board, and their authorization in representing the legal person;

5.7.2. the names of the beneficial owners of the legal person;

5.7.3. the area of activity of the legal person;

5.7.4. the details of the telecommunications.

5.8. The representative of the legal person participating in the transaction shall submit in addition to an identity document in the form provided a document certifying his or her powers.

5.9. The power of attorney issued to the representative of the legal person must include at least the following:

information of the principal (name of the competent body, registered location and registry code); – information of the representative (given name and surname, personal identification code, date of birth and place of residence); – date of issue of the document; – period of validity of the power of attorney; – the scope of the power of attorney; – right of sub-delegation, if given.

5.10. If the representative of a person participating in a transaction is a politically exposed person of another contracting state of the European Economic Area or a third country, the information on whether they are performing or have performed prominent public functions or are an associated person or a family member of the politically exposed person should also be documented.

5.11. Persons with a status of a limited partnership fund or without the status of a legal person shall be identified by applying the identification due diligence measures and, in addition, by gathering enough information to be certain that is possible to definitely identify the beneficiary at the time of making a payment or once the beneficiary exercises their rights.

**6. REGISTRATION AND PRESERVATION OF DATA**

6.1. In addition to the data specified in current procedure, the employee of H3 shall register the following data on the transaction to be performed:

6.1.1. transaction type;

6.1.2. transaction value;

6.1.3. transaction period;

6.1.4. customer account number;

6.1.5. other special conditions of the transaction.

6.2. H3 shall retain the specified data for at least five years after the performance of the transaction in a manner that allows it to immediately locate and reproduce such data.

**7. NOTIFICATION OF THE FINANCIAL INTELLIGENCE UNIT**

7.1. If H3 identifies in the process of making transactions a high-risk transaction according to chapter III, or if the person making the transaction does not submit an identity document, or if such documents are submitted but suspicions arise in regards to their authenticity or accuracy, or in case of any other failures to fulfil their obligations by the person making the transaction, the circumstances regarding the transaction shall be deemed suspicious and the transaction approached with extreme caution.

7.2. If an employee of H3 identifies in the course of an economic or professional activities or an official operation an activity or circumstances with characteristics that suggest money laundering or terrorist financing, or which they suspect or know to be money laundering or terrorist financing, they shall immediately notify the compliance officer of the company of such findings, who will, in turn, forward this information to the Financial Intelligence Unit.

7.3. H3, its structural unit, a member of the management body and an employee is prohibited to inform a person, its beneficial owner, representative or third party about a report submitted on them to the Financial Intelligence Unit, a plan to submit such a report or the occurrence of reporting as well as about a precept made by the Financial Intelligence Unit or about the commencement of criminal proceedings. H3 may inform a person that the Financial Intelligence Unit has restricted the use of the person’s account or that another restriction has been imposed after a precept made by the Financial Intelligence Unit has been complied with. The restriction specified in the current clause shall not be applied in cases specified in subsections 51 (2) and (3) of the Money Laundering and Terrorist Financing Prevention Act.

7.4. The indicators for suspicious transactions have been specified in the Guidelines on the characteristics of suspicious transactions (https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/fatf%20recommendations%202012.pdf)

7.5. The law requires obliged entities to report any transaction whereby a pecuniary obligation of over 32, 000 euros or an equal sum in another currency is performed in cash, regardless of whether the transaction is made in a single payment or in several linked payments.

7.6. The compliance officer shall attach to a filled-out report copies of documents justifying the transaction, also copies of the identification documents used to identify the person. Copies of other documents describing the nature of the transaction may be attached to the report.

7.7. The H3 employee must provide all the data requested in the order upon the first request of the Georgian Financial Intelligence Service, the tax authorities of Georgia, the Central Bank of Georgia and the credit institution in which H3 has bank accounts of any kind. In addition, H3 and its employees undertake to provide any information in response to official requests from government agencies in the United States and the European Union.

**8. COMPLIANCE OFFICER AND PERSON IN CHARGE**

8.1. The duties of a compliance officer include:

8.1.1. verification of the performance of the anti-money laundering requirements;

8.1.2. reporting to the Financial Intelligence Unit in the event of suspicion of money laundering or terrorist financing;

8.1.3. responding to any inquiries made by the Financial Intelligence Unit and complying with the precepts;

8.1.4. gathering data on suspicious and/or unusual transactions and processing and retaining such data either in a specific electronic file or on paper, including at least data on the specifics of a suspicious or unusual transaction, the person that submitted the data, the date and location of submission;

8.1.5. periodic submission of written statements on compliance with the procedure to the management board;

8.1.6. informing the management board in writing of any shortcomings in compliance with the internal audit rules, code of conduct and other legal acts.

8.2. The compliance officer has the right to:

8.2.1. check transactions and their registration in accordance with the legislation of Georgia, the European Union and the United States and the current AML policy and other local regulations of the Company;

8.2.2. during the provision of services, verify the compliance of the activity with the money laundering and terrorist financing prevention requirements.

8.3. The compliance officer may forward information that has become known to them in relation to a money laundering suspicion only to:

8.3.1. the management board and employees appointed by the management board;

8.3.2. the Financial Intelligence Unit;

8.3.3. a preliminary investigation authority in relation to criminal proceedings;

8.3.4. a court on the basis of a court ruling or judgment.

8.4. An employee shall notify the compliance officer of all cases of refusal to establish a business relationship on the basis of the Money Laundering and Terrorist Financing Prevention Act, suspicions of money laundering or unusual transactions, extraordinary terminations of long-term contracts.

8.5. The following data will be documented in a format which can be reproduced in writing on suspicious or unusual transactions:

8.5.1. description of the specifics of a suspicious or unusual transaction;

8.5.2. person(s) connected to the transaction;

8.5.3. date and location of the transaction.

8.6. The employee shall report to the Financial Intelligence Unit any transaction whereby a pecuniary obligation of over 32, 000 euros or an equal sum in another currency is performed in cash, regardless of whether the transaction is made in a single payment or in several linked payments. The specified duty to report is based on a sum and does no not depend on whether the employee had a suspicion of money laundering or not.

8.7. The report shall be submitted to the Financial Intelligence Unit orally, in writing or via electronic means of communication. Where a report was submitted orally, it will be repeated by the compliance officer the next working day in writing.

8.8. The reports compiled by the compliance officer shall be stored, used and retained similar to other data, in accordance with the aforementioned requirements of this procedure.

**9. PERSON IN CHARGE**

9.1. The duties of a person in charge include:

9.1.1. regular consultation of the website of the Financial Intelligence Unit (https://www.fms.gov.ge/eng/home/) that contains information regarding the imposition, amendment or termination of financial sanctions, in order to achieve the objective of the international financial sanction and avoid infringement of the international financial sanction;

9.1.2. verification of a new client of an individual if the transaction amount exceeds 15,000 euros, and a client of a legal entity if the transaction amount exceeds 100,000 euros, or verification of a current client of a legal entity if there have been changes in their management bodies, owners or representatives. If the customer is a legal entity, both its representative, members of the governing body, and beneficial owners must be verified.

9.1.3. review of the customer base at least once every four months.

9.2. The person in charge shall collect and retain for five years the following data:

verification date;

name of the person who performed the verification;

verification results;

applied measures.

9.3. If there is a doubt that a person who has a business relationship with or conducts a transaction or operation or is planning to establish a business relationship or conduct a transaction or operation with H3 is subjected to an international financial sanction, additional data should be requested from such person to determine whether these suspicions are true.

9.4. If a person who has a business relationship with or conducts a transaction or operation or is planning to establish a business relationship or conduct a transaction or operation with H3 is subjected to an international financial sanction refuses to provide additional data or the submitted data is not sufficient to determine whether the person is a subject of an international financial sanction, the obliged entity or their authorized representative shall refuse from making a transaction or an operation, applies measures specified in the legal act imposing or applying the international sanction and immediately notify the Financial Intelligence Unit and the management board of H3 of their suspicions.

9.5. If the activity of the person cannot be fully qualified as an activity that should be reported to the Financial Intelligence Unit in accordance with the current procedure, increased attention should be paid to any further activity of the customer. The Financial Intelligence Unit should be notified immediately if a justified suspicion about the actions of the customer arises.

9.6. Reporting to the Financial Intelligence Unit and forwarding relevant data shall not be considered a breach of a legal or contractual confidentiality obligation and the liability for the disclosure of such data established in a legal act or contract shall not be applied to the person who made the report.

**10. FINAL PROVISIONS**

10.1. The compliance officer or another employee of the institution appointed by the management board of the institution or a qualified person of the respective field shall be responsible for conducting the training of the employees on money laundering and terrorist financing prevention and international sanctions (hereinafter training).

10.2. The compliance officer shall be responsible for conducting regular trainings. Trainings shall be carried out whenever necessary but no less frequently than once a year. Every person shall confirm their participation in the training with their signature.

10.3. Respective to the established procedure, the compliance officer shall instruct new employees at least in one week after the new employee has taken up their duties and introduce this procedure to the new employee against their signature.

10.4. The compliance officer has the right to make proposals to the management board of the company about persons conducting the trainings. If a person has taken the obligation to follow the guide of conduct on the basis of an authorization agreement, they shall follow this procedure in full extent.

10.5. All documents required to carry out an inspection shall be submitted to the inspectors upon the first request of an employee of the Financial Intelligence Unit.

**11. VIOLATION OF THE DATA DOCUMENTATION AND RETENTION OBLIGATION**

11.1. Violation of the documentation and registration obligation for data specified in the Money Laundering and Terrorist Financing Prevention Act is punishable according to the relevant legislation.

Начало формы

Конец формы