ANTI-MONEY LAUNDERING POLICY, PROCEDURE AND INTERNAL CONTROL RULES OF

AVELOT LIMITED

(**"Company"**)

Registry number:
2741105

Legal address: RM 747, 7/F Star HSE 3,
Salisbury rd, Tsim Sha Tsui, Hong Kong

28th of June, 2021

Chapter I General Principles

To strengthen the anti-money laundering (“AML”) and counter terrorism financing (“CFT”) mechanisms of AVELOT LIMITED (hereinafter called “the Company”) to establish the internal control and audit framework, and to maintain the reputation of the Company and its subsidiaries, the “Anti-Money Laundering and Countering Terrorism Financing Policy of AVELOT LIMITED” (hereinafter referred to as “the Policy”) has been formulated in accordance with:

(1) The Securities and Futures Commission ("SFC") Guideline on Anti-Money Laundering and Counter- Terrorist Financing;
(2) Prevention of Money Laundering and Terrorist Financing Guideline issued by the SFC for Associated Entities;
(3) Directive (EU) 2018/843 of the European Parliament and of the Council of May, 30 2018 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directives 2009/138/EC and 2013/36/EU;
(4) Anti-Money Laundering and Counter-Terrorist Financing Ordinance, Cap. 615;
(5) United Nations (Anti-Terrorism Measures) Ordinance (UNATMO), Cap. 575;
(6) United Nations Sanctions Ordinance (UNSO), Cap. 537;
(7) Financial Action Task Force Guidance for a Risk-Based Approach to Virtual Currencies (2019).

The Rules are introduced to all employees of AVELOT LIMITED whose duties include establishment of business relationship or carrying out transactions and their monitoring.

AVELOT LIMITED shall regularly check whether the Rules are up-to-date and make necessary changes upon amendments to the regulations in force.

Chapter II Application of Customer Due Diligence Measures

The Code of Conduct for the application of customer due diligence measures is furnished to comply with the Anti-Money Laundering and Counter-Terrorist Financing Ordinance, Chapter 615, Laws of Hong Kong and applicable guidelines.

1. Purpose and Application

1.1. The purpose of this Code of Conduct is to ensure the proper identification and verification of customers, as well as ongoing monitoring of business relationships, including transactions carried out during business relationships, proper verification of data used for identification, update of relevant documents, data or information and, when necessary, identification of the source and origin of funds involved in transactions.

1.2. This Code of Conduct for the application of CDD measures includes:

1.2.1. Requirements for the identification and verification as well as methods for the collection of relevant data, including requirements for the data and documents on which the identification is based;
1.2.2. Procedures for the identification of the purpose and intended nature of business relationships and transactions prior to the execution of such transactions, and procedures for ongoing monitoring of business relationships;
1.2.3. A description of low risk transactions and requirements for and procedures of the execution of such transactions;
1.2.4. A description of high-risk transactions and requirements for and procedures of the execution and ongoing monitoring of such transactions;
1.2.5. Procedures for updating the data and documents used for identification and verification;
1.2.6. Other matters arising from the purpose and scope of the Code of Conduct.

1.3. Customer due diligence ("**CDD**") is one of the main tools for preventing money laundering and terrorist financing. CDD comprises of a set of measures and practices arising from the organisational and functional structure of the Company and described in this manual.

1.4. The purpose of CDD is to prevent the use of illegally obtained assets and property in the economic activity of the Company. CDD is based, first and foremost, on applying the Know-Your-Customer ("**KYC**") principle, under which a customer shall be identified and

respective transactions shall be assessed based on the customer's expected business activity. In addition, CDD serves to identify unusual circumstances in the customer's activity whereby an employee of the Company has reason to suspect, or has a knowledge based on facts regarding money laundering or terrorist financing.

1.5. CDD ensures the application of adequate risk management measures in order to ensure constant monitoring of customers and their transactions, as well as collection and analysis of all relevant information. Upon applying the CDD measures, the Company will follow the principles compatible with its business strategy and, based on prior risk analysis and depending on the nature of the customer's business relationships, apply CDD measures to a different extent.

1.6. CDD is applied based on a risk sensitive basis, i.e. the nature of the business relationship or transaction and the risks arising therefrom shall be taken into account upon selection and application of the measures. Risk-based CDD calls for the prior weighing of the specific business relationships or transaction risks and, as a result thereof, qualification of the business relationship in order to decide on the nature of the measure to be taken (for instance, regular, enhanced or simplified due diligence measures could be applied).

1.7. If the risk level of a customer is low, the Company may apply simplified due diligence ("**SDD**") measures but is not allowed to skip CDD entirely. If the risk level arising from a customer or a person participating in a transaction is high, enhanced due diligence ("**EDD**") measures will be applied.

1.8. Upon establishing a business relationship, the Company will identify the person and verify their right of representation based on reliable sources, identify the beneficial owner and, in the case of companies, the control structure, as well as identify the nature and purpose of possible transactions, including, if necessary, the source and origin of the funds involved in the transactions.

1.9. CDD measures are appropriate and sufficient if they allow to identify:

(1) transactions related to money laundering or terrorist financing;
(2) suspicious or unusual transactions; and
(3) transactions that do not have a reasonable business purpose, or
(4) if they at least contribute to the attainment of these purposes.

1.10. The most important requirement for the measures on prevention of money laundering and terrorist financing is that the Company shall not enter into transactions or establish relationships with anonymous or unidentified persons. Legislation requires that the Company declines the transaction or the establishment of a business relationship if:

(1) a person fails to provide sufficient information:
    a. for the identification; or
    b. about the purpose of the transactions, or;
(2) if the activity of the person involves a higher risk of money laundering or terrorist financing.

Also, legislation requires the Company to terminate a business relationship without the prior notification if the person fails to submit sufficient information for application of CDD measures.

1.11. The Company ensures that information concerning a customer (incl. collected documents and details) is up to date. When the customers or business relationships attributed to the high-risk category, the information will be updated more frequently than in the event of low or medium risk customers/business relationships. The respective data shall be stored in writing or in a form that can be reproduced in writing and made available to all relevant employees who need it to perform their employment duties (management board members, compliance officers, account managers, risk managers and internal auditors).

1.12. Independent control mechanisms are established over adherence to these procedures and the relevant training of employees are ensured.

2. Risk-Based Approach

2.1. General Requirements

The Company shall identify, assess and analyse money laundering and terrorist financing risks in its own activities and in the activities of its customers and take measures to mitigate these risks. The applicable measures shall correspond to the identified risk level.

In course of the risk-based approach, the Company shall assess the probability of risks and what the impact of their realisation is.

2.1.1. Upon identifying and assessing the risk level of a particular customer, the Company shall take into account, among other things, the following risk categories and factors:

Risk Category	**Risk Factor**
Client Risk	Whether the person is subject to international sanctions (UN, EU, OFAC, etc.).
	Whether the person is a politically exposed person ("PEP").
	Whether the person is represented by a legal person (e.g. introducer, attorney).
	Whether a third party (individual) is the beneficial owner of the transaction.
	Circumstances (including suspicious transactions identified in the course of a prior business relationship) resulting from the experience of communicating with the person, its business partners, owners, representatives and any other persons.
	The duration of the operations and the nature of business relationships.
	The type and nature of the services used or products consumed by the person outside the Company.
	The nature of the personal activities of an individual.
	Whether the origin of the person's wealth or the source and origin of the funds used for a transaction can be easily identified.
Client Risk (for legal entities only)	Turnover of the customer base
	Whether the person's customer base has increased rapidly.

	Whether the person provides its services to anonymous customers.
	The legal form, management structure, field of activity of the person, including whether it is a trust fund, civil law partnership or another similar contractual legal entity or a legal person with bearer shares.
	Whether the identification of the beneficial owner is impeded by complex and non-transparent ownership structure.
	Whether the service or product may be related to criminal activity.
	Nominal shareholders, directors, self-declared ultimate beneficial owners.
Product / Service Risk	Nature of services provided to the customer.
	Individual / account type transaction limits.
Geographical Risk	Whether the country applies legal provisions that are following the international standards of prevention of money laundering and terrorist financing.
	Whether there is a high crime rate (incl. drug-related crime rate) in the country.
	Whether the known organised crime groups exploit the country to pursue their operations.
	Whether the country engages in proliferation of weapons of mass destruction.

	Whether there is high level of corruption in the country.
	Whether international sanctions have been or are being imposed on the country.
	Whether other measures have been taken against or positions of international organisations have been expressed on the country.
	Whether the country is in United Nation sanction list
Interface / Delivery Channel Risk	Whether the person has been identified face-to-face or remotely.

Taking into account all four risk categories, the Company shall determine the risk level of the customer, e.g. whether the customer's ML/TF risk level is low, medium, high or prohibited.

2.1.2. Each risk category has its weight in overall risk score, depending on number of factors included to the risk category and their severity. For instance, residency in a high-risk country, or banking jurisdiction in the high-risk country has more impact on the risk posed, then delivery channel, etc.

2.2. Guidelines for the Low Level of Risk

2.2.1. The customer's risk level is generally considered low if there is no high risk factor in any risk category and it can therefore be claimed that the customer and its operations demonstrate elements that do not differ from those of an ordinary and transparent person; thereby there is no reason to suspect that the customer's operations may increase the probability of money laundering and terrorist financing.

2.2.2. In a situation where the application of the required measures of customer due diligence arises from legislation and information about the customer and its beneficial owner is publicly available, where the operations and transactions of the person are in line with its day-to-day economic activities and do not differ from the behaviour of other similar customers or where the transaction is subject to quantitative or other absolute restrictions,

the Company may deem the customer's estimated money laundering or terrorist financing risk to be lower.

2.2.3. In a situation where at least one risk category can be qualified as high, the risk level of money laundering or terrorist financing cannot usually be low. Equally, a low risk does not necessarily mean that the customer's operations cannot be associated with money laundering or terrorist financing at all.

2.2.4. If the risk resulting from a business relationship, a customer or transaction is low due to risk factors established with respect to the party to the transaction or the customer and the other conditions have been fulfilled, the Company may apply simplified due diligence measures, but may not omit the customer due diligence measures entirely. Upon application of customer due diligence measures by way of the simplified procedure, the Company may determine the scope of application of the customer due diligence measures.

2.2.5. For low-risk customers the Company must apply the periodic review of a business relationship less frequently than usual, including reassess the customer’s risk profile every 2 years after the establishment of the business relationship.

Criteria of Low Risk

This chapter shall not be applied if it appears from publicly available information that the risk of money laundering or terrorist financing related to a client or a transaction is not low.

General requirements for the application of simplified customer due diligence measures:

1. The Company may apply simplified customer due diligence measures (“SDD”) describing low risk criteria and establishing requirements and procedures adequate for establishing business relationship with such customers and executing their transactions.

2. The Company may consider such transactions to be low risk transactions which are not anonymous and where the obligated person is upon the suspicion of money laundering or terrorist financing able to apply immediately the customer due diligence measures.

Criteria of low risk for customers

3. Upon identification and verification of persons or customers, the following concurrent circumstances shall be considered as the criteria of low risk:

(1) the customer is a company listed on a regulated market, which is subject to disclosure obligations that establish requirements for ensuring sufficient transparency regarding the beneficial owner;
(2) the customer is a legal person governed by public law established in Hong Kong;
(3) the customer is a governmental authority or another authority performing public functions in Hong Kong;
(4) the customer is an institution of the European Union;
(5) the customer is a credit institution or financial institution acting on its own behalf or a credit institution or financial institution located in a contracting state of the European Economic Area or a third country, which in its country of location is subject to requirements equal to those established in Directive (EU) 2015/849 of the European Parliament and of the Council and subject to state supervision;
(6) a person who is a resident of a country or geographic area having the characteristics specified in points 1–4 of subsection 4 of this section.

4. Upon assessment of factors referring to a lower risk, at least the following situations where the customer is from or the customer's place of residence or seat is in, may be deemed a factor reducing geographic risks:

(1) a contracting state of the European Economic Area;
(2) a third country that has effective AML/CFT systems;
(3) a third country where, according to credible sources, the level of corruption and other criminal activity is low;
(4) a third country where, according to credible sources such as mutual evaluations, reports or published follow-up reports, AML/CFT requirements that are in accordance with the updated recommendations of the Financial Action Task Force (FATF), and where the requirements are effectively implemented.

2.3. Guidelines for the High Level of Risk

2.3.1. The customer's risk level is usually high, when assessing the risk categories on the whole it seems that the customer's operations are not ordinary or transparent; there are risk factors of impact due to which it may be presumed that the likelihood of money laundering or terrorist financing is high or considerably higher. The customer's risk level is also high if a risk factor as such calls for this. A high risk does not necessarily mean that the customer is laundering money or financing terrorists.

2.3.2. If the Company feels that the risk level of a customer or a person participating in a transaction is high, the Company shall apply customer due diligence measures pursuant to the enhanced procedure in order to adequately manage the respective risks. Thereby enhanced due diligence measures shall be applied.

2.3.3. The Company shall document the determination of the risk level, update it and make the data available to competent authorities, if necessary.

2.3.4. For high-risk customers the Company must apply the periodic review of a business relationship more frequently than usual, including reassess the customer's risk profile not later than 6 months after the establishment of the business relationship.

Criteria of High Risk

1. This chapter specifies factors referring to a higher risk of money laundering and terrorist financing in addition to the events specified in subsection 6.6 of these Rules. These factors shall be considered upon application of enhanced due diligence measures.

2. These factors shall be taken into consideration in whole or in part depending on facts and circumstances surrounding each particular customer and/or transaction.

3. The following are deemed situations increasing risks related to the customer as a person:

(1) the business relationship based on unusual factors, including in the event of complex and unusually large transactions and unusual transaction patterns that do not have a reasonable, clear economic or lawful purpose or that are not characteristic of the given business specifics;
(2) the customer is located in a high-risk country;
(3) the customer is a legal person or a legal arrangement, which is engaged in holding personal assets;
(4) the customer is a cash-intensive business;
(5) the customer is a company that has nominee shareholders or bearer shares or a company whose affiliate has nominee shareholders or bearer shares;
(6) the ownership structure of the company appears unusual or excessively complex, given the nature of the company's business.

4. Upon assessment of factors referring to a higher risk in accordance with subsection 1 of this section, in particular the following is deemed a situation increasing risks related to the product, service, transaction or delivery channel:

(1) private banking;
(2) provision of a product or making or mediating of a transaction that might favour anonymity;
(3) payments received from or sent to third parties;
(4) new products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products.

Upon assessment of factors referring to a higher risk in accordance with subsection 1 of this section, in particular as situation where the customer, a person involved in the transaction or the transaction itself is connected with a following country or jurisdiction is deemed a factor increasing the geographical risk:

(1) that, according to credible sources such as mutual evaluations, detailed evaluation reports or published follow-up reports, has not established effective AML/CFT systems;
(2) that, according to credible sources, has significant levels of corruption or other criminal activity;
(3) that is subject to sanctions, embargos or similar measures issued by, for example, Hong Kong, or the European Union or the United Nations;
(4) that provides funding or support for terrorist activities, or that has designated terrorist organisations operating within their country, as identified by Hong Kong, the European Union or the United Nations.

3. Corporate Governance Arrangements

3.1. The Board of Directors of the Company (the "**Board**") shall review the efficiency of the internal procedures implemented for the purpose of complying with the Act at least annually and ensure that internal controls are effective and in place for following the internal procedures. The Company shall appoint the person from the Board who is responsible for the application of the CDD measures. The competence and responsibilities of the person shall transparently and unambiguously arise from internal documentation regulating the tasks and functions of the members of the management board (e.g. rules of procedure of the management board, job descriptions of the members of the management board and contracts of service with the members of the management board).

3.2. The person appointed by the Board shall ensure the application of CDD measures based on regulatory requirements and that the measures are adequate and proportionate to the risk profile of the Company.

3.3. The Board ensures that the resources allocated to comply with the Act are sufficient and that the employees directly involved in the fulfilment of the requirements of the Act are fully aware of its requirements.

Conflict of interest

3.4. The Company shall mitigate and prevent conflicts of interests with internal rules, whereby the grounds of remuneration of executives and employees encourage them to disregard provisions of these Rules.

Qualifications and Training

3.6. Each director, officer and employee directly involved in the implementation of the Rules shall have professional skills that allow them to fully and with sufficient accuracy adhere to the provisions of legislation in accordance with the scope of their responsibilities and they shall have completed the respective training or been otherwise instructed therein by the Company.

3.7. The Company shall provide its vendors (including outsourcing providers) and all relevant staff, including staff whose duties include the establishment of business relationships and/or the execution of transactions and their monitoring, management of customer relationships, with regular training in and notification about the nature of the risks of money laundering and terrorist financing and any new trends in the field. First and foremost, staff shall be kept informed about the requirements governing the prevention of money laundering and terrorist financing with respect to the application of CDD measures and reporting of suspected money laundering.

4. Compliance Officer

4.1. The Board shall appoint a compliance officer for performance of AML/CFT duties and obligations. The functions of a compliance officer may be performed by an employee or member of the Board or several employees and/or a business unit with the relevant duties. If the functions of the compliance officer are performed by a business unit, the head of the relevant business unit will be responsible for the performance of the functions.

4.2. The position of a compliance officer within the Company shall allow for the performance of the requirements provided by law for the prevention of money laundering and terrorist financing. Upon establishment of the compliance officer position, the compliance officer shall be made directly accountable to the Board and made as independent from other business processes as possible.

4.3. The compliance officer's independence from business processes does not mean that the compliance officer is prohibited to advise or train colleagues for the purpose of ensuring the compliance with the requirements.

4.4. The professional qualifications and skills of the compliance officer shall meet the requirements established by SFC and the compliance officer's professional and business reputation shall be impeccable.

4.5. The duties of the compliance officer include:

- Organisation of collection and analysis of information referring to unusual transactions or transactions suspected of money laundering or terrorist financing in the activities of the Company (collection of information means collection of any and all suspicious or unusual notices received from the employees, contractual partners and agents of the Company, and analysis of the information contained in them);
- Reporting to the Joint Financial Intelligence Unit (the "JFIU") in the event of suspicion of money laundering or terrorist financing (notice being given in the manner agreed with the JFIU);
- Periodic submission of written statements on implementation of the rules of procedure to the Board; and
- Performance of other obligations related to the fulfilment of the AML/CFT requirements of the Hong Kong Special Administrative Region (including training employees and applying respective control mechanisms).

4.6. The compliance officer shall have access to the information used for establishing a business relationship, including any information, data or documents reflecting the identity and business activity of the customer. The management board also grants the compliance officer the right to participate in the meetings of the management board if the compliance officer deems this necessary to perform their functions.

4.7. The contact details of the compliance officer shall be communicated to the Financial Intelligence Unit. The compliance officer shall inform the Financial Intelligence Unit within

a reasonable term about the appointment of a new compliance officer or a change in contact details.

5. Outsourcing

5.1. The Company has the right, considering special requirements and restrictions provided by law, to use the services of a third party under a contract the subject of which is the continuing performance of activities and continued taking of steps required for the provision of services by the Company to its customers and that would normally be performed and taken by the Company itself. For the purposes of this section, third parties include, for instance, agents, subcontractors and other persons to whom the Company transfers the activities relating to the provision of the services provided as a rule by the Company in its economic activities.

5.2. The Company shall choose the third party in order to ensure the ability of the person to fulfil the regulatory requirements and to ensure the reliability and the required qualifications of such a person.

5.3. The third party specified in section 5.1 is subject to all of the requirements provided by law for prevention of money laundering and terrorist financing regarding outsourced activities. The Company who outsourced its activities is liable for infringement of the requirements.

5.4. Upon outsourcing of any activities, the Company shall ensure that the third party has the knowledge and skills required, above all, for the identification of situations of a suspicious and unusual nature and is able to meet all of the requirements for the prevention of money laundering and terrorist financing provided by law. To comply with the provisions in this section, the Company shall ensure the notification of the executives of the third party of the relevant requirements and the training of its staff in the prevention of money laundering and terrorist financing.

5.5. Upon outsourcing of any activity to third parties, the Company shall ensure that any documents and information collected for the fulfilment of requirements arising from legislation are preserved in accordance with the procedure established in the Act and any legislation issued on the basis thereof. The contract shall ensure that relevant information is handed over to the Company and that the relevant information and documents are archived in accordance with its rules of procedure.

5.6. The outsourcing contract shall specify the rights and duties of the Company upon reviewing compliance by the third party with the requirements provided by law. The outsourcing of economic activities to a third party shall not impede state supervision over the Company and the latter shall, under contract, grant competent authorities access to the third party for supervisory purposes to whom the Company has outsourced its duties, tasks or functions.

5.7. Whilst services are provided by third parties, situations where the application of customer due diligence measures to the required extent is possible to an insufficient degree or entirely impossible shall be avoided. A third party shall be able to fully apply the required customer due diligence measures, thereby being able to notify the contact person of the Company immediately and to decline a transaction. The Company shall, under contract, ensure its right to terminate the contract with the third party if the latter fails to perform its contractual duties or obligations or performs the unduly.

6. Customer Due Diligence Measures

6.1. The Company applies customer due diligence measures upon:

6.1.1. establishment of business relationship;
6.1.2. verification of information gathered while applying due diligence measures or in the case of doubts as to the sufficiency or truthfulness of the documents or data gathered while updating the relevant data;
6.1.3. suspicion of money laundering or terrorist financing, regardless of any derogations, exceptions or limits provided for in these Rules and/or the Law.

6.2. The Company applies the following CDD measures:

6.2.1. identification of a customer and verification of the submitted information based on information obtained from a reliable and independent source, including using means of electronic identification and of trust services for electronic transactions;
6.2.2. identification and verification of a customer's representative and their right of representation;
6.2.3. identification of the beneficial owner and, for the purpose of verifying their identity, taking measures to the extent that allows the obliged entity to make certain that it knows who the beneficial owner is, and understands the ownership and control structure of the customer – legal entity or arrangement;
6.2.4. understanding of business relationships and, where relevant, gathering information thereon;

6.2.5. gathering information on whether a person is a politically exposed person, their family member or a person known to be close associate;
6.2.6. monitoring of a business relationship.

6.3. The Company shall, in addition to the CDD measures listed above, comprehensively evaluate the nature and purpose of the customer's transactions and actions, relying on the universally recognised professional skills characteristic of credit institutions and financial institutions to identify a possible link between a transaction, step or funds and money laundering or terrorist financing.

6.4. The Company has sufficiently applied the CDD measures if it is convinced that it has sufficiently applied the obligation arising from the aforementioned provision. The principle of reasonableness is considered upon assessing conviction.

6-1. Simplified Due Diligence Measures

6-1.1. The obliged entity may apply simplified due diligence ("**SDD**") measures where a risk assessment prepared on the basis of Section 2 of these Rules identifies that, in the case of the economic or professional activity, field or circumstances, the risk of money laundering or terrorist financing is lower than usual.

6-1.2. Before the application of SDD measures to a customer, the Company establishes that the business relationship or a particular transaction is of a lower risk.

6-1.3. The application of SDD measures is permitted to the extent that the Company ensures sufficient monitoring of transactions, and business relationships, so that it would be possible to identify unusual transactions and allow for notifying of suspicious transactions in accordance with the procedure established these Rules.

6-2. Enhanced Due Diligence Measures

The Company applies enhanced due diligence ("**EDD**") measures in order to adequately manage and mitigate a higher-than-usual risk of money laundering and terrorist financing.

6-2.1. EDD measures are applied always when:

(1) upon identification of a person or verification of submitted information, there are doubts as to the truthfulness of the submitted data, authenticity of the documents or identification of the beneficial owner;

(2) the customer is a politically exposed person ("PEP"), their family member or a close associate;
(3) the customer is from a high-risk country or their place of residence or seat or the seat of the payment service provider is in a high-risk country;
(4) the customer is from such country or territory or their place of residence or seat or the seat of the payment service provider is in a country or territory that, according to credible sources such as mutual evaluations, reports or published follow-up reports, has not established effective AML/CFT systems that are in accordance with the recommendations of the Financial Action Task Force, or that is considered a low tax rate territory.

6-2.1. The Company applies EDD measures also where a risk assessment prepared on the basis of Section 2 of these Rules identifies that, in the case of the economic or professional activity, field or factors, the risk of money laundering or terrorist financing is higher than usual.

6-2.3. When EDD is required, the Company applies one or several of the following measures:

(1) verification of information additionally submitted upon identification of the person based on additional documents, data or information originating from a credible and independent source;
(2) gathering additional information on the purpose and nature of the business relationship, or transaction and verifying the submitted information based on additional documents, data or information that originates from a reliable and independent source;
(3) gathering additional information and documents regarding the actual execution of transactions made in the business relationship in order to determine the economic purpose of the transaction;
(4) gathering additional information and documents for the purpose of identifying the source and origin of the funds used in a transaction made in the business relationship;
(5) require the senior management approval.

6-2.4. Information required for applying EDD measures shall be collected through the completion of the AML questionnaire on the website. The questionnaire requires the following information to be provided:

(1) Self-certification on a US person status;
(2) Self-certification on a PEP status (including family member and close associate);
(3) Link to social networks;
(4) Employment status;
(5) Source of funds and wealth (including cryptocurrency);
(6) Monthly income;
(7) Destination of cryptocurrency;
(8) Primary banking jurisdiction;
(9) Purpose of the account (establishing of business relationship);
(10) Intended amount of monthly deposit.

7. General Requirements for Identification of Individuals

7.1. The identification and verification of the identity of an individual (a natural person) shall be carried out on the basis of information provided by the customer, an identity document and a document confirming residential address of the customer.

The customer has to provide the following set of data upon identification:

(1) Full name;
(2) Date of birth;
(3) Country of birth
(4) Gender
(5) Citizenship
(6) Email address
(7) Phone number
(8) Identity document information
(9) Residential address

7.2. The Company identifies a customer - natural person - based on the following documents:

(1) Passport; or
(2) ID card.

7.3. The customer also is required to provide a selfie with the ID document and face to face verification if the monthly transaction higher then required by law, which serves as an additional level of security against identity theft, and helps to mitigate interface risk.

7.4. A document submitted to the Company for identification shall be assessed as follows:

- validity of the document based on the date of expiry;
- the outward likeness and age of the person match the appearance of the person represented on the document;
- the personal identification code matches the gender and age of the submitter; and
- with respect to information contained in codes assigned to individuals of a foreign country, foreign missions or other competent authorities shall be consulted in the case of doubt as to the authenticity of the document or identity.

7.5. The copy of the document shall be of a quality allowing the details included on it to be clearly readable.

7.6. The Company shall verify the residential address of the customer on the basis of the one of the following documents:

- Utility bill
- Electricity bill
- Bank statement (including credit card statement)
- Council Tax Return
- Other document issued by a regulated entity stating the residential address and the name of the customer

7.7. The Company may record other contact details, social network accounts, Skype account and other similar data.

7.8. Determining field of activity, job or profession gives the Company the opportunity to assess whether the business relationship or transactions are in compliance with the customer's normal participation in commerce and whether the business relationship or transaction has a clear economic reason. For the purpose of prevention of the movement of illegally acquired funds, the customer's operating profile needs to be identified upon reaching specific transaction threshold. To this end, the customer's main fields of work and activity and possible transaction habits need to be identified.

7.9. Upon identifying an individual, it shall be identified whether the person is a politically exposed person.

7.10. Any details and references required to identify a person shall be verified by means of reliable and independent sources of information (e.g. national registers, authorities, credit institutions, foreign missions in the Hong Kong Special Administrative Region or based on documents and other information certified by other relevant authorities). In exceptional instances (if the use of reliable and independent sources of information is impossible), copies of documents or information communicated by unofficial representatives or mediators or other dependable information (incl. handwritten statements by a person) may be relied on to identify a person. The Company shall, prior to entering into transactions or taking steps with the person to be identified, make certain that the information obtained in such a manner is sufficient. In such an instance, a notation to this effect shall be made on the copies confirming identification, and thereafter the legality of the details and documents shall be verified immediately.

7.11. The recommendation of a person by the executives, other customers or business partners of the Company may contribute to the identification of the customer, but the respective recommendations do not substitute for the identification requirements and do not release the Company from the fulfilment of the requirements.

7.12. Even if the Company knows the customer personally or the customer is a public figure, the internal identification procedure provided by these Rules cannot be disregarded. The identity of the public figures and persons directly or indirectly related to them who address the Company for performance of transactions or taking of steps shall be verified.

7.13. The Company shall regularly update the customer's personal data and operating profile, ensuring that they are up to date and based on the customer's risk level.

7.14 Upon identifying an individual, the Company shall, in the event of doubt, also identify the beneficial owner of the individual, i.e. the person who controls the actions of the individual.

7.15. A doubt about the existence of a beneficial owner may arise, above all, if the Company perceives, upon applying customer due diligence measures, that the individual has been forced to establish the business relationship or enter into the transaction. In such an event the person who exercises control over the individual shall be deemed the individual’s beneficial owner.

7.16. It shall be considered that the scope of customer due diligence, including upon identifying the beneficial owner, is related to the risk of money laundering and terrorist financing, which depends on the type of customer, its country of origin, business relationship, product, service or transaction.

8. Politically Exposed Persons

8.1. Individuals who have, or have had, a high political profile, or hold, or have held, public office, can pose a higher money laundering risk to the Company as their position may make them vulnerable to corruption. This risk also extends to members of their immediate families and to know close associates. PEP status itself does not, of course, incriminate individuals or entities. It does, however, put the customer, or the beneficial owner, into a higher risk category. The Company shall imply EDD to PEPs.

8.2. A PEP is defined as an individual who is entrusted with prominent public functions, other than as a middle-ranking or more junior official.

Individuals entrusted with prominent public functions include:

- Heads of state, heads of government, ministers and deputy or assistant ministers;
- Members of parliaments or of similar legislative bodies;
- Members of supreme courts, of constitutional courts or of other high-level judicial bodies the decisions of which are not subject to further appeal, except in exceptional circumstances;
- Members of courts of auditors or of the boards of central banks;
- Ambassadors, charges affairs and high-ranking officers in the armed forces (other than in respect of relevant positions at Community and international level);
- Members of the administrative, management or supervisory boards of State-owned enterprises; and
- Directors, deputy directors and members of the board or equivalent function of an international organization.

Family members of PEPs:

- The spouse, or a person considered to be equivalent to a spouse of a PEP;
- The children and their spouses, or persons considered to be equivalent to a spouse, of a PEP; and
- The parents of a PEP.

Persons known to be close associates of PEPs:

- Natural persons, who are known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations, with a PEP; and
- Natural persons who have sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de-facto benefit of a PEP.

Public functions exercised at levels lower than national should normally not be considered prominent. However, when their political exposure is comparable to that of similar positions at national level, for example, a senior official at state level in a federal system, firms should consider, on a risk-based approach, whether persons exercising those public functions should be considered as PEPs.

8.3. The following EDD measures in addition to the general CDD measures should be applied to PEPs

- obtains approval from the senior management to establish or continue a business relationship with the person;
- applies measures to establish the origin of the wealth of the person and the sources of the funds that are used in the business relationship;
- designation of custom transaction limits based on a verified source of funds/wealth;
- monitors the business relationship in an enhanced manner.

8.4. Where a PEP is no longer entrusted with a prominent public function either by a country or an international organization, the Company must, for at least 12 months after ceasing to be so entrusted, take into the continuing risk posed by that person and to apply appropriate and risk-sensitive measures until such time at that person is deemed to pose no further risk specific to PEPs.

9. General Requirements for Identification of Legal Entities

9.1. Data Collected from Legal Entities

9.1.1. Upon establishing a relationship with a legal entity, the following information shall be collected and verified:

(1) Full legal and trade name;
(2) Company number

(3) Legal form
(4) Legal status
(5) Legal address,
(6) Controlling persons and their legal capacity
(7) Authorised representatives (other than controlling persons) and their legal capacity
(8) Shareholders and ultimate beneficial owners (UBO);
(9) Purpose of account
(10) Expected activity on the platform
(11) Source of entity's funds;
(12) Other information which may be required for conducting identification and verification of the legal entity.

9.1.2. Upon determining the location of a legal entity for risk assessment purpose, both the country of incorporation and the physical address (premises) shall be used to identify whether the legal entity may involve country and geographical risks.

9.1.3. The physical address of a legal entity shall be determined on the basis of factual circumstances, i.e. where production is based, or a service is provided.

9.1.4. The identification and verification of the identity and legal capacity of a legal entity shall be carried out, as a general rule, on the basis of the information contained in the commercial register or another equivalent register or a copy of the registration certificate or an equivalent document (for instance, in countries where there is no national register, foundation documents certified by a notary are considered equivalent) submitted in accordance with the procedure provided by law. Documents issued by a register or their equivalents shall have been issued no earlier than 6 months prior to their submission to the Company (expect foundation documents, such as Memorandum and Articles of Association, Partnership Agreement, Certificate of Incorporation, etc.).

9.1.5. Documents issued in a foreign state shall be legalised or apostilled, i.e. in order to use an official document issued in one country in another, an internationally recognised certificate of the authenticity of the document is given in another. The documents certified by attorneys or accountants are deemed acceptable for purpose of identification and verification.

9.1.5.1. To be legalised, a document shall go through the legalisation authorities of the issuing state as well as those of the receiving state (usually, foreign ministries).

9.1.6. Upon identification, legal entities are not required to submit an extract of their registry card if the Company has access to the required extent via the Internet to the data in the commercial register or register of non-profit organisations and foundations (including access to data in respective registers in the foreign country).

9.1.7. Upon identification of a legal entity, the Company is required to register the names of the executive of the legal person or members of its management board or another body substituting for it, their powers in representing the legal entity and the principal field of activity of the legal entity. If the aforesaid details are not indicated by the register extract or another relevant document, the relevant information shall be obtained by using other documents and/or reliable sources of information.

9.1.8. The need for use, the criteria of use and/or the list of reliable sources of information shall be specified by the Company (e.g. information issued by national registers, public authorities, credit institutions, foreign missions in the Hong Kong Special Administrative Region may be used).

9.1.9. The Company shall identify the existence of politically exposed persons related to the legal entity. If no respective links appear in the information about a politically exposed person obtained from the representative of the legal entity, an enquiry shall be made with the respective databases in the event of suspicion.

9.1.10. In the case of international organisations, the documents serving as the basis for their activities (including in Hong Kong) shall be determined and the submission of relevant documents shall be requested. If necessary, information required for the establishment of the business relationship which is contained in the documents shall be verified.

9.2. Identification of Legal Entity Beneficial Ownership

9.2.1. Upon the identification of a legal entity, the Company shall identify and verify beneficial owners of the legal entity, who own 25% or more shares/interest in this legal entity.

9.2.2. In a situation where no person holds or identifiably controls more than 25%, the circle of beneficial owners will be identified pursuant to the principle of proportionality, according to which information shall be requested about the shareholders, partners and other persons who exercise control or other significant influence over the activities of the legal entity.

9.2.3. If the identification documents of a legal entity or other submitted documents do not indicate the beneficial owner of the entity, the relevant information (including information about membership of the group of companies and the ownership and management structure of the group of companies) shall be registered on the basis of the statements or a handwritten document of the representative of the legal entity.

9.2.4. In order to verify information identified on the basis of statements or a handwritten document, reasonable measures shall be applied (e.g. the filing of a query with relevant registers) and the submission of the annual report or another relevant document of the legal entity shall be requested.

9.2.5. The Company may use a risk-based approach and take sufficient measures to verify the identity of the beneficial owner with the aim of making certain as to whom the beneficial owner in the business relationship or transaction is. With respect to compliance with this requirement, the Company is left with several options in order to decide:

(1) the extent to which public information about shareholders or members will be used;
(2) the extent to which relevant information will be requested orally or to record obtained information in writing or in a form that can be reproduced in writing;
(3) in which cases the customer will be asked to complete a respective questionnaire; or
(4) what other options can be used and are practicable in the event of the Company.

9.2.6. It shall be taken into account that the scope of customer due diligence with respect to the customer (incl. identification of the beneficial owner) is related to the risk of money laundering and terrorist financing, which depends on the type of customer, their country of origin, business relationship, product, service and transaction.

9.2.7. Higher attention shall be paid to companies founded in territories with a low tax rate, whose beneficial owners are often difficult to identify.

9.2.8. The Company can consider a person who exercises control in another manner, without having a 25% shareholding in the company, as the beneficial owner. This situation arises when the Company suspects that a third party whose links to a company cannot be legally proven or are difficult to prove the exercises of control over management of a legal person.

9.3. Relationships with Shell Banks

The Company is not allowed to establish or continue correspondent or any other contractual relationships with shell banks and such credit institutions or financial institutions that knowingly allow shell banks use their accounts.

'Shell bank' means a credit institution or a financial institution, or an institution that carries out activities equivalent to those carried out by credit institutions and financial institutions, incorporated in a jurisdiction in which it has no physical presence, involving meaningful mind and management, and which is unaffiliated with a regulated credit or financial group.

10. Transaction Monitoring

10.1. Monitoring and identifying of unusual and suspicious transactions is an important part of customer due diligence measures applied by obliged entities, that allows to identify the circumstances that may point to money laundering or terrorist financing in the activity of customers. Also, the purpose of transaction monitoring is to identify transactions with subjects of international sanctions and politically exposed persons and detect and notify of transactions whose limit or other parameters exceed the prescribed value over a certain period of time.

10.2. Transaction monitoring measures can be divided into two categories: screening and analysis.

10.3. Transaction screening allows transactions to be monitored in real time, based on data accompanying the transaction. The following "red flags" may be identified upon transaction screening:

- politically exposed persons involved in transactions;
- transactions with persons whose name, alias, date of birth or other identifiable information match with data in lists of persons subject to international sanctions, adverse media, enforcement actions, etc.;
- payments received from or sent to a high-risk country;
- payment received from or sent to a third-party (non-customer of the Company)

10.4. Transaction analysis helps to detect deviations in customer's activity and identify unusual transaction patterns which may be related to money laundering, terrorist financing or other illegal activity. The following red flags may be identified upon transaction analysis:

- single large international payments (e.g. whereby the sum ends with at least four zeros);
- accounts with the highest turnover in the period under review based on currencies;
- the largest transactions in the period under review based on different currencies;
- single transaction that exceed the limit, which are made by customers whose turnover is small;
- sudden increase in account activity without rationale;
- transactions in multiple currencies;
- cryptocurrency transactions linked to suspicious addresses;
- transactions without apparent lawful or business purpose.

10.6. If the customer is regularly unable to give the requested information about the nature of transactions or their purpose, the Company shall take measures which include giving warnings and setting time limits. Thereafter the customer may be denied to execute any transaction or business relationships may be limited or terminated.

11. Suspicious Activity Monitoring and Reporting

11.1. In a situation where the Company, based on documents collected in the course of application of customer due diligence measures, develops a suspicion of money laundering or terrorist financing upon the establishment of a business relationship, the Company shall not establish the business relationship.

11.2. If unusual circumstances or circumstances whereby an employee of the Company suspects money laundering or terrorist financing become evident in relationships with a customer, the compliance officer appointed by the management board shall be immediately informed thereof and the compliance officer will decide the immediate forwarding of the information to the JFIU and the need to postpone or refuse to make the transaction. In a situation that entails a high risk of money laundering or terrorist financing, an employee of the Company may decide to postpone the transaction and thereafter inform the compliance officer of the situation.

11.2.1. The background of each individual suspect or unusual instance shall be investigated as much as reasonably necessary, thereby recording the details of the transaction and analysing the circumstances with the aim of identifying the typical features of more frequent transactions.

11.2.2. The main circumstances to which attention should be paid when suspect and unusual transactions are analysed are as follows:

- What is suspicious about the steps, transactions or other circumstances?
- Is the Company convinced that it knows its customer sufficiently or is it necessary to collect additional information about the customer?
- Upon taking a step or making a transaction involving identifying a customer or the customer's representative, the Company shall make certain that it follows the prescribed procedure. Was all the required information submitted or additional information need to be requested or otherwise clarified?
- Have there been repeated instances of suspicious steps and transactions?

11.3. If the delay of a transaction could cause significant losses to the parties, its omission is impossible or may prevent the interception of the potential perpetrator of money laundering or terrorist financing, the transaction shall be performed and thereafter a report shall be forwarded to the JFIU.

11.4. The rules of procedure of the Company shall set out a code of conduct for the staff of the Company regarding the delay of a transaction.

11.5. The rules of procedure of the Company shall set out both the conditions for the forwarding of information to the JFIU as well as for the preservation of the forwarded information.

11.6. The Company shall preserve in a form that can be reproduced in writing all of the information received from staff about suspicious or unusual transactions and any information collected to analyse these reports and other related documents and any reports forwarded to the JFIU along with information about the time of the forwarding of the report and the employee that forwarded it.

11.7. No customer or party participating in a transaction (including its representative or other related parties) with respect to whom suspicion is being communicated to the JFIU may be notified of this.

11.8. The Company shall immediately fulfil the reporting obligation. The purpose of immediate fulfilment is to give the JFIU the chance to develop the suspicion and for taking its own measures. Money laundering is a process where criminal proceeds, above all, financial assets may be transferred via credit institutions and financial institutions of

multiple states in a single day and therefore swift reporting helps to track down illegal funds more effectively.

Chapter III Reporting of Money Laundering and Terrorist Financing

The Code of Conduct for the reporting of money laundering and terrorist financing is prepared to comply with the legal acts of the Hong Kong Special Administrative Region and applicable guidelines.

1. Reporting in Event of Suspicion of Money Laundering or Terrorist Financing

1.1. Where the Company identifies in its daily business an activity or facts which characteristics refer to the use of criminal proceeds or terrorist financing or to the commission of related offences or an attempt thereof or with regard to which the Company suspects or knows that it constitutes money laundering or terrorist financing or the commission of related offences, the Company must report it to the Joint Financial Intelligence Unit immediately, but not later than within two working days after identifying the activity or facts or after getting the suspicion.

1.2. Where the Company suspects or knows that terrorist financing or money laundering or related criminal offences are being committed, the execution of the transaction must be postponed until the submission of a report based on subsection 1.1 of this section. Where the postponement of the transaction may cause considerable harm, it is not possible to omit the transaction or it may impede catching the person who committed possible money laundering or terrorist financing, the transaction will be carried out and a report will be submitted the Joint Financial Intelligence Unit immediately thereafter.

2. Place and Form of Performance of Duty to Report

2.1. Information concerning suspicious activity/transaction shall be forwarded to the Hong Kong Joint Financial Intelligence Unit.

2.2. A report shall be submitted electronically.

2.3. The data used for identifying the person and verifying the submitted information and, if any, copies of the documents are added to the report.

3. Confidentiality of Report

3.1. The Company, a structural unit of the Company, a member of a 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 Joint Financial Intelligence Unit, a plan to submit such a report or the occurrence of reporting as well as about a precept made by the Joint Financial Intelligence Unit. After a precept made by the Joint Financial Intelligence Unit has been complied with, the Company may inform a person that the Joint Financial Intelligence Unit has restricted the use of the person's account or that another restriction has been imposed.

3.2. The Company may provide information to a third party if:

3.2.1. the third party belongs to the same consolidation group or financial conglomerate as the Company and the undertaking is located in third country where requirements equal to those provided in this Rules are in force, state supervision is exercised over fulfilment thereof and requirements equal to those in force in Hong Kong are applied for the purpose of keeping professional secrets and protecting personal data;

3.2.2. the third party acts in the same legal person or structure, which has joint owners and a joint management or internal control system, as the Company who pursues the profession of a notary public, attorney or auditor;

3.2.3. the information specified in subsection (1) concerns the same person and the same transaction which is related to several Company and the information is given by a credit institution, financial institution, notary public, attorney or auditor to a person operating in the same branch of the economy or profession and located in third country where requirements equal to those provided in this Rules are in force, state supervision is exercised over fulfilment thereof and requirements equal to those in force in Hong Kong are applied for the purpose of keeping professional secrets and protecting personal data.

4. Relief From Liability

4.1. The Company, its employee, representative or a person who acted in its name shall not, upon performance of the obligations arising from the Rules, be liable for damage arising from failure to enter into a transaction or failure to enter into a transaction by the due date if the damage was caused to the person participating in the transaction made in economic or professional activities in connection with reporting of the suspicion of money laundering or terrorist financing to the Joint Financial Intelligence Unit in good faith, or for damage caused to a customer or a person participating in a transaction entered into in economic or professional activities in connection with cancellation of a contract entered into for an indefinite period.

4.2. The performance in good faith of the reporting arising from communication of relevant data by the Company is not deemed infringement of the confidentiality requirement provided by law or contract and no liability provided by legislation or contract is imputed with regard to the person who performed the notification obligation for disclosure of the information.

5. Guidelines of Joint Financial Intelligence Unit

5.1. The Joint Financial Intelligence Unit issues advisory guidelines to explain legislation regulating the prevention of money laundering and terrorist financing which is available on its website https://www.jfiu.gov.hk/en/.

5.2. The Joint Financial Intelligence Unit issues advisory guidelines regarding the characteristics of suspicious transactions which is available on its website.

5.3. The Joint Financial Intelligence Unit issues advisory guidelines regarding the characteristics of terrorist financing which is available on its website.

Internal Audit

1. The tasks of Internal control rules are:

1.1. to verify compliance of the Company and its managers and employees with the legislation and guidelines of the Joint Financial Intelligence Unit, decisions of the management bodies, internal rules, contracts and good practices concluded by the Company.

1.2. in cooperation with all the management levels of the Company, to identify and assess the risks that may affect the effectiveness of the Company's activities and its internal control system, determine the priorities of its activities and draw up work plans on the basis of the results of the risk assessment;

1.3. to assess the management and control measures implemented to achieve the Company's objectives, their effectiveness, sustainability and effectiveness, and express an opinion on the adequacy, reliability and necessity of these measures;

1.4. to inform the management board of its findings and conclusions and, if necessary, make recommendations for remedying the situation, modifying measures or implementing new ones;

1.5. as a result of the aforementioned activities, to increase the Company's management's confidence that the management and control measures implemented are aimed at achieving the goals set by the Company are sufficient and not superfluous.

2. The task of the Board of Directors is to appoint a person responsible for the internal control of the Company ("**internal auditor**") and, if necessary, to establish a respective internal unit leading by the internal auditor, ensure the necessary conditions for the work of the internal unit, access to the necessary information and the independence from the Company's other units and departments, and implement, as far as possible, proposals.

3. In order to ensure the independence of the internal control function, the internal auditor shall not be involved in the duties that affect the outcome of an internal audit.

4. The internal auditor shall be independent in the planning of his/her activities.

5. The internal auditor shall be independent in carrying out audits, making observations, conclusions and recommendations, and informing the results, and maintaining neutrality with regard to the auditee.

6. Internal auditor requirements:

6.1. An internal auditor may be a natural person:

(i) who may not serve in the position and perform other duties which cause or may cause a conflict of interest;

(ii) who has impeccable reputation, honesty and high moral qualities, and who has the capabilities and personal qualities necessary for the work of the internal auditor;

(iii) having higher education.

6.2. The internal auditor is guided by the rules of conduct contained in internationally accepted standards.

6.3. The internal auditor ensures that the audits are carried out professionally and with due diligence, in accordance with applicable legislation and internationally accepted standards.

7. Risk Assessment, Audit Planning and Audit:

7.1. There is a risk that an event, activity or omission can cause loss of the assets or reputation of the Company and jeopardize the effective performance of the tasks assigned to the Company. The purpose of internal control is, among other things, to prevent the realization of risks, which will be achieved by fulfilling the work plan based on the results of the risk assessment.

7.2. Risk assessment for the purposes of these Rules is a process aimed at identifying risks in the Company and prioritizing those changes that are necessary in the strategic audit plan, and preparing an annual work plan for an audit.

7.3. All the management levels of the Company and the person responsible for internal control must be involved in the risk assessment.

7.4. Risk assessment is carried out at least once a year before the audit work plans are drawn up.

7.5. An audit work plan is prepared for the planning of internal audit work.

7.6. The company's audit work plan is prepared by the internal auditor and approved by the Board of Directors.

7.7. The audit work plan shall be prepared at the beginning of each year and shall state:

(1) the results of the risk assessment;
(2) audit objects and objectives;
(3) the planned deadline for completion of each audit by quarter.

7.8. The audit work plan must be based on the results of the risk assessment, take account of the operational priorities set for them and the resources available for internal audit, and leave a reasonable reserve to perform one-off tasks coming from the Company's management board.

7.9. An audit plan is prepared by the internal auditor. The audit plan must contain the following information:

(1) the purpose of the audit;
(2) the name of the audited entity or sector;
(3) the scope of the audit and the period covered;
(4) the time of the audit.

7.10 The audit involves audit planning, audit activity, final report preparation and reporting of results and, if necessary, ex-post audits.

7.11. The audit object may be any of the Company's structural units, systems, processes, operations, functions and activities.

7.12 The internal auditor must be guaranteed access to the information necessary for conducting the entire audit in the Company.

7.13. The internal auditor shall be guaranteed all the rights and working conditions necessary for the performance of his duties, including the right to receive clarifications and information from the managers and employees of the Company, and to monitor the elimination of the deficiencies found and the implementation of the proposals made.

7.14. Internal audit is carried out at least annually.

8. Preparation and submission of a report:

8.1. At the end of each audit, the internal auditor will draw up an audit report, which will outline the findings, conclusions and recommendations for modifying the situation based on evidence contained in the audit dossier made during the audit.

8.2. The internal auditor shall forward the final report to the management board of the Company and, if necessary, to other management staff.

8.3. When reporting breaches of law, the internal auditor must comply with applicable laws and internationally accepted standards.

8.4. The Internal Auditor is required to promptly forward information to the Company's managers about the information disclosed to him about the violation of the law, or to the detriment of the interests of the clients.

9. Audit documentation and procedures:

9.1. Any information obtained during the audit, which is the basis for making conclusions and making recommendations, assessing risks and planning future audits, must be documented.

9.2. In order to ensure the high quality of the audit and to enable a later understanding of the audit process, all documents obtained during the audit and the prepared working papers must be included in the audit file. The dossier must ensure that the documents are easily accessible by reference in the final report and elsewhere.

9.3 The organization of internal control, the establishment and maintenance of audit dossiers must be guided by the laws and regulations governing the Company's current rules and procedures.