



✉ INFO@KAURI.FINANCE
🌐 [LINKEDIN: KAURIFINANCE](https://www.kauri.finance)
📌 [TELEGRAM: @KAURI.FINANCE](https://t.me/@KAURI.FINANCE)

[WWW.KAURI.FINANCE](https://www.kauri.finance)

KAURIFINANCE OÜ

Narva mnt 7B, 10117 Tallinn, Estonia
Triumph Plaza, office 519
Registry code: 14559136
License #FVT000328

ANTI-MONEY LAUNDERING AND COUNTERING TERRORISM FINANCING POLICY

Last review: February 2021



✉ INFO@KAURIFINANCE
🌐 LINKEDIN: KAURIFINANCE
📧 TELEGRAM: @KAURIFINANCE

WWW.KAURIFINANCE

KAURIFINANCE OÜ

Narva mnt 7B, 10117 Tallinn, Estonia
Triumph Plaza, office 519
Registry code: 14559136
License #FVT000328

CONTENT

PREAMBLE	3
1. DEFINITIONS.....	3
2. SCOPE OF APPLICATION.....	4
3. PRINCIPLES.....	4
4. ROLES AND RESPONSIBILITIES	7
5. KEY PROCESSES	8
6. CLIENT DUE DILIGENCE.....	9
7. RISK PROFILING OF THE CLIENT/COUNTERPARTY.....	10
8. SUSPICIOUS TRANSACTION MONITORING	12
9. GOVERNANCE.....	13
10. VALIDITY DATE AND PERIODIC REVIEW	14
APPENDICES.....	15
Annex 1. KNOW YOUR CUSTOMER FORM.....	15
Annex 2. FATF High-risk and other monitored jurisdictions 2019	24
Annex 3. Indicators of money laundering.....	26

PREAMBLE

Kaurifinance OU is an innovative company in the proprietary algorithmic trading industry. The business model of the Company does not involve the attraction of funds from outside persons, both individuals and legal entities, and is based solely on the conduct of all trade operations at the expense of the company's own funds.

Nevertheless, subject to the requirements of regulations and rules of exchange platforms, the Company has developed these rules in order to meet all the requirements of regulators and the best international standards in the field of doing business and combating money laundering.

The purpose of this Policy is (i) to establish the principles and standards that must be adhered by Kaurifinance OU (hereinafter referred to as the "Company") in relation to the prevention and control of money laundering and terrorist financing (hereinafter referred to as the "AML Policy"), and also for the purposes of compliance with international sanction programmes, (ii) to define roles and responsibilities in this area, (iii) to establish the policies and procedures that must be undertaken by the Company and (iv) to define the essential features of the governance.

1. DEFINITIONS

The following definitions are established for the purposes of this Policy:

- ✓ **Counter-terrorism fighting (CTF):** financial countermeasures against the illegal smuggling of cash to terrorist organizations.
- ✓ **Estonian Financial Supervision and Resolution Authority** is a financial supervision and crisis resolution authority with autonomous responsibilities and budget that works on behalf of the state of Estonia and is independent in its decision-making.
- ✓ **International sanction and programs:** Instruments of a political, diplomatic and economic nature used by international institutions and countries to exert influence in areas such as the prevention and pursuit of terrorism, support and defence of human rights and civil liberties, deterrence of possible armed conflicts or the prohibition of the development of weapons of mass destruction.
- ✓ **Money laundering (ML):** Participation in any activity that has the aim of acquiring, possessing, controlling, using, converting, transferring, concealing or disguising the nature, source, location, disposition, movement or rights with respect to, or ownership of, criminal property in the knowledge that that property is the proceeds of criminal activity or participation in such activity.
- ✓ **Terrorist financing (TF):** The provision, deposit, distribution or collection of any property, in any means, directly or indirectly, with the intention that the property be used, or knowing that the property will be used, in whole or in part, to commit a terrorist act.
- ✓ **The Financial Action Task Force (FATF)** is an inter-governmental body established in 1989 by the Ministers of its Member jurisdictions. The objectives of the FATF are to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. The FATF is therefore a "policy-making body" which works to generate the necessary political will to bring about national legislative and regulatory reforms in these areas.

The Office of Foreign Assets Control (OFAC) of the US Department of the Treasury administers and enforces economic and trade sanctions based on US foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy or economy of the United States. OFAC acts under Presidential national emergency powers, as well as authority granted by specific legislation, to impose controls on transactions and freeze assets under US jurisdiction. Many of the sanctions are based on United Nations and other international mandates, are multilateral in scope, and involve close cooperation with allied government.

Money laundering and terrorist financing are universal globalised phenomena that take advantage of the international economy and the gradual elimination of barriers to trade globally, calling for a coordinated global response by the international community and the financial sector to prevent the sector being used for illicit purposes. The Company recognises the importance of the fight against money laundering and terrorist financing as it affects essential aspects of social life. The Company will always fully cooperate with the relevant authorities in this area.

This Policy has been developed based on the following legislative acts:

- ✓ the Estonian Money Laundering and Terrorist Financing Prevention Act (MLTFPA);
- ✓ the Procedure for the registration and processing of data collected by the Financial Intelligence Unit;
- ✓ Criteria of low risk of money laundering and terrorist financing which allows the application of simplified customer due diligence measures;
- ✓ Anti-money laundering - Directive (EU) 2018/843;
- ✓ Anti-money laundering - Directive (EU) 2015/849;
- ✓ and other relevant and applicable to the Company international legislation.

2. SCOPE OF APPLICATION

This Policy:

- ✓ is applicable throughout the whole Company, is applied on a mandatory basis and compliance with it must be evidenced;
- ✓ shall be adopted by the Board of Directors of the Company;
- ✓ shall be adhered to by the Company with any adaptations being strictly limited to those required by local law and regulation. Any adaptation or waiver for any part of this framework must be limited to those required by local law and regulation and submitted to the Company for consideration and approval;
- ✓ includes reference to specific elements for local implementation all of which should be submitted to the Company for validation to ensure they are consistent with this Policy. This should also be subject to periodic review and updates.

3. PRINCIPLES

The following principles reflect the minimum Company's expectations of the AML Policy as a whole. These principles are mandatory and must be applied at all times.

- ✓ **Assessment and management of business risk:** All Company's branches and/or departments if any will be classified by levels of risk for the purposes of designing and implementing measures and controls to mitigate such risks, and for applying greater supervision to high-risk areas of business, products and channels. This acknowledges that the risk of involvement in money laundering or terrorist financing is directly related to the type of business carried on by the Company or their branches, the products they

distribute, and the channels used. It also considers that this threat may be managed more efficiently if there is prior knowledge of the potential risk concerning the various types of business and products.

- ✓ **Customer risk segmentation, Identification and Know Your Customer:** Customers of the Company if any must be classified by risk level for the purposes of designing and implementing measures and controls to mitigate these risks, and for applying greater control over high-risk customers and transactions. This acknowledges that the risks inherent to money laundering may be managed more efficiently if there is prior knowledge of the potential risk concerning the various types of customers and transactions.
- ✓ Counterparties and transactions must be monitored on a continuous basis once such counterparties have established a formal relationship with the Company.
- ✓ Know Your Customer obligations (hereinafter referred to as the "KYC") to identify (and know your customer and their activities) must be established by appropriate due diligence. This obligation will be met in accordance with the provisions made by the applicable legislation and the risk level in areas of business, activities, products, services, distribution or sales channels, countries of operation and transactions carried out.
- ✓ **Prohibited counterparties with enhanced acceptance measures:** The Company will not accept counterparties where the necessary data is not available, or which fall into one of the Company agreed categories of prohibited counterparties. Prohibited counterparties are as follows:
 - Persons on official sanctioned lists or persons that are related to¹ countries prohibited by the Company in the terms determined.
 - Persons where information is available to suggest that they may be involved in criminal activities.
 - Persons with businesses the nature of which makes it impossible to verify the legitimacy of the activities or the origin of the funds.
 - Persons who refuse to provide the information or documentation required.
 - Legal where the shareholder structure or control structure cannot be determined.
 - Casinos or gambling companies that are not officially authorised.
 - Financial institutions that are registered in countries or territories in which they do not have a physical presence (also known as "shell banks").
 - Counterparties on the list of prohibited customers in the Company's corporate policies.

The following categories of customers will only be accepted with prior authorisation by the internal governance body responsible for anti-money laundering and financing of terrorism²

- Counterparties involved with the production or distribution of weapons and other military products.
- Casinos or gambling companies officially authorised.
- Foreign exchange companies, money transmission companies or similar.

¹ That have a link to the prohibited country or to individuals or legal resident or incorporated in the prohibited country or are related to the government or the official institutions of the state (even if they are resident outside the prohibited country).

² The most senior management committee in relation to AML/CTF.

³ Under MLTFPA PEPs are a) individuals who are or have been entrusted with prominent public functions by a foreign country, such as head of State or head of government; minister, deputy minister or assistant minister; member of a legislative body; member of a governing body of a political party; judge of the highest court of a country; auditor general or a member of the supervisory board or executive board of a central bank; ambassador, envoy or chargé d'affaires; high-ranking officer in the armed forces; member of an administrative, management or supervisory body of a state-owned enterprise; director, deputy director and member of a management body of an international organisation.

⁴ a) a spouse (including a person who is considered by national law to be equivalent to a spouse; b) a partner; c) children and their spouses or partners; d) siblings and e) parents (including in-laws where this can be ascertained). 'Known close associates' include: a) A person who is a joint is the sole beneficial owner of an arrangement set up for the benefit of a PEP

- Politically exposed persons (PEPs)³ and their and their relatives and close associates⁴.
- ✓ **Transaction monitoring and analysis:** Ongoing monitoring of a business relationship with all types of customers must be conducted, controlling and analysing sensitive or high-risk transactions in connection with money laundering and terrorist financing, in order to detect suspicious transactions.
 Proper IT systems must be available to this end, taking into consideration the type of transactions, business sector, geographic environment and transactional volume.
 Enhanced monitoring must be applied to material high-risk counterparties and transactions, according to the key indicators in respect of these counterparties and their accounts, considering circumstances as countries of origin, the origin of funds, the type of transactions and other risk factors.
- ✓ **Suspicious transaction reporting and systematic reporting:** The Company must fulfil the obligation of reporting and cooperate with the relevant authorities.
 The Company ensures that all employees are aware of their obligations to immediately report potentially suspicious transactions to the internal AML function, in order to, in accordance with the law, make the necessary reviews and report or notify suspicious transactions to the authorities if required by the law.
 The Company ensures that all employees are aware of their obligations when reporting a potentially suspicious transaction or activity to the internal AML function, including not to provide any information, internally or externally, on concerned counterparties or transactions.
 The Company ensures that the blocking of transactions and movement of funds and/or the prohibition of opening accounts is executed in line with local law and regulation.
- ✓ **Recordkeeping:** The Company ensures that robust record-keeping is maintained and that, as a minimum, documents listed below are kept for a period of at least five (5) years as required MLTFPA regulations or any longer periods where applicable:
 - Documentation regarding identifying and knowing your customers/counterparties.
 - Reports submitted to the authorities concerning the suspicious activities of a customer/ counterparties in connection with potential money laundering and/or terrorist financing, along with any supporting documentation.
 - Registers of training on money laundering and terrorist financing (Annex 2).
 - Any other documents or registers that must be kept by applicable legislation of anti-money laundering or terrorist financing.
- ✓ **AML/CTF Training:** All employees receive ongoing training on the obligations arising from regulations on the anti-money laundering and terrorist financing. This is facilitated through:
 - Annual trainings to managers and employees and specifically staff performing those jobs that, by nature, are suitable for detecting any events or transactions that may be related to money laundering or terrorist financing, enable the employees to carry out detection and know how to proceed in such cases.
 - The registration of all trainings, with a description of the main characteristics and contents.
 - Continual sharing of information to all those responsible for anti-money laundering in all business of any regulatory changes in this area, as well as any new systems, techniques or procedures detected that may be used for money laundering or terrorist financing.

³For the purposes of this Policy, considering the requirements of the operations threshold the amount of 10 000 USD or more will be acceptable for AML Procedure

⁴For the purposes of this Policy, considering the requirements of the operations threshold the amount of 10 000 USD or more will be acceptable for AML Procedure

Sanction programs: The Company has effective policies and procedures in place in order to effectively comply with the restrictions under sanction programs and international financial countermeasures.

The Company identifies and follows sanction programs and financial countermeasures, monitors the international sanction programs issued by UN, EU and OFAC that might affect the activities of the Company.

The Company assesses risks and manages to determine the extent to which a business relationship or activity may be affected by international restrictions, and approach must be taken into account in risk assessment methodology.

The Company refrains from conducting business relationships with restricted persons and no direct or indirect relations shall be established with persons who are subject to international restrictions. To this end, appropriate and up to date knowledge of counterparties, their activity, and other persons and carrying on relationships with the Company should be obtained.

The Company maintains commercial operations and payments in compliance with regulations. Transactions carried out by the Company must be compliant with the restrictions under international sanction programs, and no transactions can be undertaken if they fail to meet the conditions set out in the programs.

The Company implements internal controls and prevention mechanisms. Controls and specific measures must be implemented for the prevention and detection of deficiencies in systems and negligent or irregular action taken by employees that may result in a failure or malfunctions in the application of international restrictions.

- ✓ **Consolidated management of know-your-customer risks:** Consolidated management of know-your-customer risk constitutes a principle for coordinating and sharing information throughout the Company that helps identify, monitor and reduce risks, and comply with applicable legislation and regulations.

The Company must immediately provide the parent company, if any, with appropriate data concerning high-risk customers and activities and react promptly to information requests by the parent company to assist the Company to manage regulatory and reputational risk relating to money laundering and terrorist financing. This may include data protection laws and cross-border utilisation, depending on the jurisdiction.

The Company establishes the same above-mentioned discipline for local units/subsidiaries or subsidiaries in third-party jurisdictions, if any, that are directly controlled by them in relation to AML/CTF.

The Company, in all cases, establishes safeguard mechanisms so that information concerning counterparties and their transactions are kept strictly confidential, subject to privacy laws in the country of origin.

4. ROLES AND RESPONSIBILITIES

The following is a description of the roles and responsibilities of functions involved in the matters covered by this Policy. Such roles and responsibilities are exercised respecting the three lines of defence.

The Company has an appropriate organizational and governance structure to identify, prevent and detect money laundering and terrorist financing, report in line with the requirements established in law, and block or freeze funds or economic resources following application of controls of sanctions or international financial countermeasures.

The Company has at least one person appointed as a head the function level, who will take responsibility for application of this framework, its implementation, and enter into dialogue with local supervisors if necessary.

The Company may appoint special Compliance Officer who will be responsible for AML/CTF in specific business areas, which operate under the coordination and dependency of the anti-money laundering and terrorist financing function.

- **First line of defence:**

As a general rule and in the context of AML/CFT, the business and support units are the first line of defence in charge of identifying, assessing and controlling the risks of their business. They should know and carry out the policies and procedures such as KYC and risk management procedures and be allotted sufficient resources to do this effectively. As part of the first line of defence, policies and procedures are clearly specified in writing, and communicated to all personnel. They should contain a clear description for employees of their obligations and instructions as well as guidance on how to keep the activity of the Company in compliance with regulations. There should be internal procedures for detecting and reporting suspicious transactions.

- **Second line of defence:**

Risk and Compliance & Conduct, as the second line of defence, will provide independent challenge and oversight of the risk management activities performed by the first line of defence. This second line of defence ensures that risks are managed in accordance with the risk appetite defined by senior management and promote a strong risk culture throughout the organization as noted in the GBP- 7. Kaurifinance OU Risk management Policy.

As an independent second line of defence, the risk management and compliance function is responsible for monitoring and overseeing risks arising from AML/TF and sanction programs, assessing the impact on risk appetite and the risk profile of the Company and taking account of the provisions of this framework. They will develop and implement the necessary updates to the present policy and AML procedures to properly manage and control the prevention of money laundering and terrorist financing and sanction programs.

The risk management function is responsible for integrating and consolidating the risks arising from conduct and reputational risks, assessing the impact on risk appetite and the risk profile of the entity, and taking account of the provisions of this framework. They also add conclusions to specific risk information in such a way as to present a complete picture of the full range of risks to which the entity or the Company is exposed.

- **Third line of defence:**

As part of the third line of defence, the Internal Audit Function regularly assesses that policies, methods and procedures are adequate and effectively implemented for the management and control of the system for the prevention of money laundering and terrorist financing for compliance with sanction programs in the Company, providing an independent assessment.

5. KEY PROCESSES

The Company has an effective internal procedure in place enabling to demonstrate that the AML/CTF activities and related processes are properly executed and are in line with all applicable laws and regulations including sanction programs and international financial countermeasures.

To be in compliance with these obligations, the Company has an appropriate procedure for the prevention of ML and TF and ensuring their effectiveness and compliance with all relevant legal and regulatory requirements:

- (a) Adopts and changes procedures, where applicable, for dealing with ML and TF reflecting the current statutory and regulatory requirements;
- (b) ensures that the content of this Policy is relevant and understood by all staff members;
- (c) regularly reviews the policies and procedure to ensure their effectiveness (at least once a year);
- (d) adopts client acceptance policies and procedures (Annex 1);
- (e) undertakes client due diligence (CDD) measures to an extent that is sensitive to the risk of ML and TF depending on the type of client, business relationship or transaction;
- (f) identifies, monitors and reports suspected ML or TF transactions to the law enforcement authorities.

The Company may also issue additional documents to act as guidelines for the proper interpretation and consistent application of internal policies within the Company where it deems applicable.

Internal regulations drawn up by the Company are validated for the prevention of money laundering and terrorist financing before they are approved by the most senior local management committee in relation to AML/CTF.

Specifically, the Company must have the procedures in place that cover the following mandatory areas:

- (a) prevention of money laundering and terrorist financing, and specifically covering certain activities of Clients if any (Annex 1).
- (b) supervision and assessment of the risks arising from management and prevention of money laundering and terrorist financing and compliance with international sanction programs which should be reflect in the relevant GBP-7. Kaurifinance OU Risk Management Policy.

6. CLIENT DUE DILIGENCE

In case if the Company will engage any client's operations and deal with any counterparties the following rules for Clients Due diligence will be applicable⁵:

- Obtain sufficient information about the client in order to identify who is the actual beneficial owner or on whose behalf transaction is conducted.
- Verify the customer's identity using reliable, independent source document, data or information (for example, verification of clients' registration from the relevant State web site, etc).

Customer Due Diligence Process includes following specific parameters:

- Procedure for Clients Acceptance;
- Risk based approach;
- Client Identification Procedure;
- Client classification based on risk category.

Client Acceptance Procedures

- (a) Do not accept clients with identity matching persons known to have criminal background: The Company inquires the clients whether they have criminal background or are not banned in any other manner, whether in terms of criminal or civil proceedings or by any enforcement/regulatory agency worldwide. If yes, such clients are not accepted.
- (b) Do not accept clients with identity matching with banned person/entity as per relevant Stock Exchanges in capital market in any jurisdiction where the Company has its business: check whether the client's identity matched with persons debarred/banned by any Stock Exchange before any business relations. If yes, such counterparties are not accepted.
- (c) If monies from a counterparty are accepted, each such client/counterparty should be met in person: perform the in-person verification process very diligently. Either the client should visit the Company's office or concerned official/employees may visit the client at their residence/office address. Officials/employees also verify photocopy of the documents with the original. If the counterparty was referred to by another existing Company's counterparty the introducer detail would be set in account opening form.
- (d) Accept clients/counterparties on whom we are able to apply appropriate KYC procedures:
 - Obtain complete identification information from the client. It should be ensured that the initial forms taken by the client are filled in completely.
 - All photocopies submitted by the client should be checked against original documents

⁵For the purposes of this Policy, considering the requirements of the operations threshold the amount of 10 000 USD or more will be acceptable for AML Procedure

without any exception.

- 'Know Your Client' guidelines should be followed without any exception.
- Where possible, the Company identifies the ultimate beneficial owners of the counterparties. The identification procedure includes obtaining reliable data on persons who are the final beneficiaries and exercising control and/or ownership of assets / shares / corporate rights of legal entities directly or via the chain of mediated owners.
- The counterparty provides the Company with information on the entire chain of owners and discloses data on final beneficiaries who own not less than 10% of property rights in the company⁶, or submit a corresponding document confirming that such identification is not possible if the company is managed by trust funds, has a significant amount of minority shares. owners, etc.
- Do not compromise on submission of mandatory information/ documents: business relationships should be started only upon receipt of all mandatory information along with authentic supporting documents as per the regulatory guidelines. Where the counterparty refuses to provide information/documents business relationships should not be continued.
- The Company should capture data of key persons like director & shareholder of all non-individual counterparties and also taking complete details/documents of Director/Trustee/Partners etc., which is mandatory while granting the services or making other business relationships. In case of a corporate client in order to identify client with cross holding, we capture key persons' data, for example, details of director, shareholders.

Special attention should be paid while accepting clients/counterparties of the special categories listed below:

- Trust,
- Charities,
- NGOs,
- Politically Exposed Persons (PEP),
- Companies having close shareholding/ beneficial ownership,
- Clients in high risk countries (e.g. Libya, Somalia, Afghanistan, etc., according to special list of high-risk jurisdictions as set in Annex 2),
- Non-face to face clients,
- Clients with dubious background,
- Clients belonging to countries where corruption/fraud level is high (e.g. Nigeria, Burma, etc., according to the special list for specific jurisdictions as per Transparency International).

Scrutinize the records / documents pertaining to clients belonging to aforesaid categories.

- Check if the client identity is in the lists of FATF, OFAC. Try to match the name/identity number from the available information from these lists. If we find any client name in these lists, then we should inform to Special authority in the relevant Exchange jurisdiction immediately & do not start cooperation with such a client as a requirement for security dealers.

7. RISK PROFILING OF THE CLIENT/COUNTERPARTY

The Company should accept the clients/counterparties based on the risk they are likely to impose. The aim is to identify clients who are likely to bear a higher than average risk of money laundering or terrorist financing. For this purpose, the Company classifies the clients as low risk, medium risk and high-risk clients. By classifying

⁶ For the purposes of this Policy, considering the requirements of the legislative regulations, the minimum amount of ownership of a company for identification as a UBO is 10% of shareholder / ownership rights, etc.

the clients, we will be in a better position to apply appropriate customer due diligence process. That is, for high risk client the Company has to apply higher degree of due diligence.

Special attention is to be paid to the transactions which are complex, unusually large or pattern which appears to have no economic purpose. Risk profiling is divided into two broad categories: on-board risk assessment and ongoing risk assessment.

In order to achieve this objective, all clients should be classified in the following category:

- **Category A - Low Risk:** At the time of business cooperation all clients other than special category clients will be marked as Low risk client.
- **Category B - Medium Risk:** To enhance the due diligence of a client who initially falls in low risk category & has abnormal transaction pattern. Depend on the pattern a client can be shifted to medium risk category or high-risk category directly.
- **Category C - High risk:** Any client falls in special category mentioned above at the time of business cooperation will be considered as High risk and as a part of identifying ongoing risk, other clients which come under review & found high risk due to their transaction pattern will be marked as high risk.

The various factors which are considered while marking a client as Medium/High Risk are (1) Percentage of volume in exchange is very high & amount in absolute term is substantial and/or (2) High volume transactions, Illiquid or such other high risk stock and/or (3) a Client who does not have financial status aligned with its transaction volume and/or (4) a Client having abnormal transaction pattern. Then an alert is created to classifying as Medium/High Risk category. But classification is being done after looking at the other qualitative criteria also.

8. SUSPICIOUS TRANSACTION MONITORING AND REPORTING

The Company analyzes the suspicious transactions on a routine basis.

Suspicious transaction means a transaction, which to a person acting in good faith -

- Gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime; or
- Appears to be made in circumstance of unusual or unjustified complexity; or
- Appears to have no economic rationale or bona fide purpose.

8.1. Reasons for Suspicion

➤ Identity of a client/counterparty

- a) False identification documents
- b) Identification documents which could not be verified within reasonable time
- c) Non-face to face client
- d) Clients in a high-risk jurisdiction
- e) Doubt over the real beneficiary of the account
- f) Business transactions are similar or very close to the business identification (name, address, etc.) of other established business entities

Policy: Generally, the Company starts business cooperation only after ensuring that identity of a client is valid and genuine.

8.2. Suspicious Background

➤ Suspicious background or links with criminals

Policy: Generally, the Company starts business cooperation only after ensuring that a client does not fall under list of entities issued by the relevant authority in relevant Jurisdiction or United Nations Sanctions List.

Accordingly, the Company takes an evidence for source of income. As well as, checks shareholding pattern and list of Director of a counterparty to establish the person behind the company. In our client registration form, we insist our client to provide us the details of his/her annual income range as per IT return/salary slip, etc. Source of finance is essential for a counterparty who wants to trade in derivative segment. On a routine basis, we monitor the client volume in scrip with exchange volume.

8.3. What to Report

In any case the Company has to report the following information in the desired format to relevant state authority in respect of suspicious transactions:

- The nature of the transactions
- The amount of the transaction
- The date on which the transaction was conducted
- The parties to the transaction
- The reason of suspicion
- Details of person who have made such transactions.

At the request of the relevant authorities, if such a request is provided for in accordance with the current legislation, the Company undertakes to provide any other available information on suspicious transactions.

8.4. Reporting Procedure

In general, as a Estonian legal entity, the Company should report to Money Laundering Report Office (MROS) (being the national Financial Intelligence Unit in ESTONIA (FIU)) if knows or has reasonable grounds to suspect that assets involved in the business relationship:

- are the proceeds of a felony or of an aggravated tax misdemeanor;
- are connected to money laundering or to a criminal organisation which pursues the objective of committing crimes of violence or which aims at financial gain by criminal means
- serve the financing of terrorism
- are subject to the power of disposal of a criminal organisation; or
- are related to persons contained on 'terrorist lists'.

If the Company filed a SAR it must not inform the concerned person or any third parties of the report; SROs and FIU do not constitute third parties for the purpose of the information ban (article 10a AMLA).

- 8.4.5. If in the process of identifying and researching of the counterparty it is determined that the counterparty, by any of the identifying criteria, is included in the list of persons for whom prohibitive and or sanctional measures in accordance with the requirements of the financial regulators, FATF, OFAC, etc., the Company applies the following procedures:
- (a) An employee of the Company who discovered the AML violation notifies the Compliance officer about the fact that the counterparty's profile does not comply with the requirements of the AML, indicating where the specific violations were found.
 - (b) The Compliance officer notifies CEO and Board of Directors on the identified potential violations. After discussion, the Board and CEO take appropriate course of actions and if the case is classified as the one to be reported under respective AML legislation the following below steps are taken.
 - (c) The client receives a written reasoned refusal from the Company in further cooperation until the client removes all the reasons for the violation of AML requirements.
 - (d) In case the revealed violations give all reasonable grounds to assume that they fall under the valid criminal law in this case, the Client is not informed of the grounds for ceasing interaction with him.
 - (e) The Compliance Officer immediately, but in any case, no later than next three business days contacts MROS or other corresponding department of the AML in the relevant jurisdictions where this client is registered and reports the fact that the counterparty's profile does not comply with the AML requirements. If necessary, all data collected in the process of identifying such a counterparty shall be transmitted, upon request, to the competent AML control authorities, and
 - (f) The Compliance Officer immediately, but in any case, no later than next three business days contacts the corresponding department of the AML in the relevant exchange platform on which this client is registered / or wanted to register and reports the fact that the counterparty's profile does not comply with the AML requirements. Applicable to clients where the Company only acting as a security dealer. If necessary, all data collected in the process of identifying such a counterparty shall be transmitted, upon request, to the competent AML control authorities.

9. GOVERNANCE

The Governance applied in the Company promotes efficient governance structures that ensures adequate participation by all relevant functions.

The governance bodies for the Company are to be structured taking into account local regulatory and legal requirements, as well as the size and complexity of each subsidiary, if any, whilst ensuring that they are consistent with those of the parent company. Any such governance bodies must promote clear and effective decision-making and clarity of accountability.

Carrying out the AML/CTF function properly in terms of decision-making, supervision and control requires a governance structure, which can provide a response in an efficient and agile manner at both a corporate and subsidiary level if applicable.

In its application of this Policy, the Company shall identify the governance bodies or committees responsible for defining, monitoring, controlling and overseeing the AML/CTF regulatory risks.

The Company's Board of Directors and its committees if applicable, in accordance with the provisions of its Articles of Incorporation and relevant Board's regulations, are the most senior decision-making and monitoring bodies in connection with the management and control of money laundering and terrorist financing and compliance with the sanction program, except in the case of issues reserved for the general meeting.

The Boards of subsidiaries (if any) are also the most senior bodies at their level if applicable.

The Board of the Company are responsible for the:

- ✓ Adoption of Corporate AML Policy;
- ✓ Supervision of compliance with AML/CTF regulations and legislation, including any actions and measures as a result of inspections by supervisory and control authorities, in addition to internal control and assurance functions.

The risk supervision body is responsible for:

- ✓ Assisting and advising the Board in the definition and assessment of the policies stipulated in this Framework.
- ✓ Assisting the Board with supervision of the application and analysis of the place in the risk profile.
- ✓ Monitoring and assessing any regulatory proposals and new applicable regulations, and the potential consequences for the Company.

10. VALIDITY DATE AND PERIODIC REVIEW

This Policy is effective on the Company's wide basis from the date of its publication.

Its contents will be reviewed periodically, and any changes or modifications will be made as appropriate.



✉ INFO@KAURIFINANCE
 🔗 LINKEDIN: KAURIFINANCE
 📧 TELEGRAM: @KAURL.FINANCE

WWW.KAURI.FINANCE

KAURIFINANCE OÜ

Narva mnt 7B, 10117 Tallinn, Estonia
 Triumph Plaza, office 519
 Registry code: 14559136
 License #FVT000328

APPENDICES

Annex 1. KAURIFINANCE OU KNOW YOUR CLIENTS FORM

Please write clearly in block capitals. If you have any queries, please contact us on telephone No: +_____.

1 Registered details of the Company

Full Company name ("the Company")

Registered Office

Registered number:

Street / No.

Date of incorporation: ____ / ____ / ____
 (dd/mm/yyyy)

Town/City

Postcode

Country of incorporation

Country

Number of employees:

Telephone
 E-mail address

2 Communication with the Company

Correspondence Address

Company Contacts

Street / No.

Management Contact

Postcode

Town/City
 Telephone

Country

E-mail address

Telephone
 E-mail address

Company web-site:

3 Status of the Company

Is the Company regulated by the Financial Authority in its country or other country equivalent, or listed/quoted on a major Stock Exchange?

YES

☐

NO

☐

If 'YES' please give name of Financial Regulator / Stock Exchange:

Authorisation number (if applicable):

Country of Regulator / Stock Exchange:

Is the Company's ultimate beneficial owner regulated or listed/quoted on a major Stock Exchange?

YES

☐

NO

☐

If 'YES' please give the name of Regulator / Stock Exchange:

Authorisation number (if applicable):

Country of Regulator / Stock Exchange:

4 Directors of the Company

Details of all directors of the Company:

Name of Director	Position



✉ INFO@KAURI.FINANCE
🌐 LINKEDIN: KAURIFINANCE
📧 TELEGRAM: @KAURI_FINANCE

WWW.KAURI.FINANCE

KAURIFINANCE OÜ

Narva mnt 7B, 10117 Tallinn, Estonia
Triumph Plaza, office 519
Registry code: 14559136
License #FVT000328

5 Ownership of the Company

Shareholder details of the company:

Name of Shareholder	Ownership Percentage

Shareholders who are corporate entities

If any shareholder is a corporate entity please provide a breakdown of the individual shareholdings of that company in the table below, along with a corporate group structure:

Name of Shareholder / Corporate Entity	Ownership Percentage

6 Tax Residency Self-Certification

Country of Residence for Tax Purposes and related Taxpayer Identification Number or functional equivalent ("TIN")

Please complete the following table indicating (i) where the Company is tax resident and (ii) the Company's TIN for each Reportable Jurisdiction indicated.

If a TIN is unavailable please provide the appropriate reason A, B or C where appropriate:

Reason A – The country where I am liable to pay tax does not issue TINs to its residents Reason B – The Company is otherwise unable to obtain a TIN or equivalent number

Reason C – No TIN is required (*Note. Only select this reason if the domestic law of the relevant jurisdiction does not require the collection of the TIN issued by such jurisdiction*)

Country of Residence	TIN	If no TIN available enter Reason A, B or C

Please explain in the following boxes why you are unable to obtain a TIN if you selected Reason B above.

7 Company Financials

Is the company intended to request for purchase of product at open account or credit line basis?

YES

NO

☐
☐

If 'YES' please provide a copy of the latest audited Report and Accounts of the Company, if unavailable then please provide unaudited management accounts.

Please note if you cannot provide audited or unaudited financials then you will need to provide verification of the financial position of the Company.



✉ INFO@KAURI.FINANCE
🌐 LINKEDIN: KAURIFINANCE
📧 TELEGRAM: @KAURI.FINANCE

WWW.KAURI.FINANCE

KAURIFINANCE OÜ

Narva mnt 7B, 10117 Tallinn, Estonia
Triumph Plaza, office 519
Registry code: 14559136
License #FVT000328

8 The Company's principal banks details (alternatively please attach your standard settlement instructions)

Bank One:

Full name of Bank:

Name of Bank Account:

Full Address:

A/C No.:

SWIFT / IBAN No.:

Country

Bank Two:

Full name of Bank:

Name of Bank Account:

Full Address:

A/C No.:

SWIFT / IBAN No.:

Country

9 Legal Entity Identifier ("LEI") (all entities, regardless of jurisdiction of incorporation/establishment)

Please tick the box the applies below:

☐ We have an LEI or have applied for one Please provide your LEI or pre-LEI below:

☐ We do not have an LEI

Please state what your plans are for obtaining an LEI:

Important note(s): An LEI is an alphanumeric code which is 20 characters long, and is issued by a Local Operating Unit ("LOU") in return for a fee. For the avoidance of doubt, it is not a company registration number or the equivalent.

10 Principal Activities of the Company

Please, provide a brief summary description of the Company's principal activities including location of main operating entities and clients, geographical split of clients and products if available, products traded:

11 Declarations and Signature of the Company

The following officers, being duly authorised to do so, declare and confirm on behalf of the Company the following:

- I certify that I am authorised to sign for the Company in respect of all the information to which this form relates.
- the Company confirms that all statements made in this declaration are correct and complete.
- the Company undertakes to advise Kaurifinance OU immediately of any change in circumstance which causes the information herein to become incorrect (including any changes to the information on controlling persons).
- the Company acknowledges that the information contained in this form may be reported to the tax or other authorities of Switzerland and exchanged with tax authorities of another country or countries in which the Company may be tax resident pursuant to intergovernmental agreements to exchange financial account information with the country/ies in which this account(s) is/are maintained.
- the Company agrees to be bound by any provisions included in this form.

Executed by the Company acting by its duly authorised representatives Full name of Company:	
Signature	
Name (Print)	
Position / Title	Date
Signature	
Name (Print)	
Position / Title	Date
Signature	
Name (Print)	
Position / Title	Date
<div style="text-align: right;">Company Seal / Stamp</div>	

Should Kaurifinance OU and the Company enter into an agreement this form and the information set out in it will constitute part of the contract.

Please ensure that the documents listed below are provided with the completed KYC form:

- A copy of the Company's Certificate of Incorporation (or local equivalent).
- A copy of the Company's Memorandum and Articles of Association (or local equivalent).
- Copies of documents confirming the Company's ownership structure (e.g. share registers, share certificates and list of current directors).
- Proof of identity for each of the major beneficial owner(s)/ shareholders and Directors of the Company. This should include a copy of their current passport or identity card.
- A copy of the latest audited Report and Accounts of the Company, is "YES" in clause 7. (if unavailable then please provide unaudited management accounts).
- Bank references



✉ INFO@KAURI.FINANCE
🌐 LINKEDIN: KAURIFINANCE
📧 TELEGRAM: @KAURI.FINANCE

WWW.KAURI.FINANCE

KAURIFINANCE OÜ

Narva mnt 7B, 10117 Tallinn, Estonia
Triumph Plaza, office 519
Registry code: 14559136
License #FVT000328

Appendix 1 to KYC form – Controlling Persons Form

****For use by Controlling Persons of entities or trusts that are NOT financial institutions and that are not US entities only****

Controlling Persons Form - Country of residence for tax purposes

1. Legal name of prospective Kaurifinance OU Counterparty of which you are a Controlling Person

2. Name of Controlling Person completing this form

3. Current Residence Address

4. Date of birth

5. Place of birth (please specify the town/city & country)

6. Country of Residence for Tax Purposes and related Taxpayer Identification Number or functional equivalent ("TIN")

Please complete the following table indicating (i) where the Company is tax resident and (ii) the Company's TIN for each Reportable Jurisdiction indicated.

If a TIN is unavailable please provide the appropriate reason A, B or C where appropriate:

Reason A – The country where I am liable to pay tax does not issue TINs to its residents Reason B – The Company is otherwise unable to obtain a TIN or equivalent number

Reason C – No TIN is required (Note. Only select this reason if the domestic law of the relevant jurisdiction does not require the collection of the TIN issued by such jurisdiction)

	Country of Residence	TIN	If no TIN available enter Reason
1			
2			

Please explain in the following boxes why you are unable to obtain a TIN if you selected Reason B above.

1	
2	

5. Type of Controlling Person (Please tick the applicable statement(s) below)

- ☐ Controlling Person of a legal person – **control by ownership**
- ☐ Controlling Person of a legal person – **control by other means**
- ☐ Controlling Person of a legal person – **senior managing official**

6. Declarations and Signature

- I certify that I am the Controlling Person of the Company to which this form relates.
- I acknowledge that the information contained in this form and information regarding the Controlling Person and any Reportable Account(s) may be reported to the tax authorities of the country in which this account(s) is/are maintained and exchanged with tax authorities of another country or countries in which I, the Controlling Person, may be tax resident pursuant to intergovernmental agreements to exchange financial account information.
- I confirm that all the details given in this form are correct and complete.
- I will inform Kaurifinance OU immediately in writing of any changes to the details contained herein.

Should Kaurifinance OU and the prospective Counterparty enter into an agreement this form and the information set out in it will constitute part of the contract

Annex 2.

Estonia Sanction list:

<https://www.sanctionsmap.eu/#/main>

FATF High-risk and other monitored jurisdictions 2021

Afghanistan
Belarus
Bosnia & Herzegovina
Burundi
Central African Republic
China
Democratic Republic of the Congo
Egypt
Guinea
Guinea-Bissau
Haiti
Iran
Iraq
Lebanon
Libya
Mali
Moldova
Montenegro
Myanmar (Burma)
Nicaragua
North Korea
Russia
Serbia
Somalia



✉ INFO@KAURI.FINANCE
🌐 LINKEDIN: KAURIFINANCE
📧 TELEGRAM: @KAURI.FINANCE

WWW.KAURI.FINANCE

KAURIFINANCE OÜ

Narva mnt 7B, 10117 Tallinn, Estonia
Triumph Plaza, office 519
Registry code: 14559136
License #FVT000328

South Sudan
Sudan
Syria
Tunisia
Turkey
Ukraine
United States
Venezuela
Yemen
Zimbabwe

Relevant OFAC High-risk and other monitored jurisdictions and persons list could be find at:
<https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx>

Annex 3. Indicators of money laundering

1 Meaning of these indicators

1.1 Personal which are responsible for AML procedure shall take into consideration the following indicators which flag a high-risk business relationship or transaction. Just the indicators alone may not be sufficient grounds for suspicion of a money-laundering transaction subject to punishment, but the concurrence of several elements could be a strong indicator for money laundering.

1.2 A client's declaration on the background of a particular transaction must be tested for its plausibility. What is important is that not all declarations made by clients are to be taken at face value.

2 General indicators:

2.1 Transactions bear a heightened risk of money laundering if:

- ✓ their structure indicates an illegal purpose, or their economic purpose is not discernable or that it may even seem absurd from an economic point of view;
- ✓ assets which are drawn down shortly after they have been deposited at the financial intermediary (interim account), unless this is plausible in view of the client's business activities;
- ✓ it makes no sense that a client would have chosen precisely this financial intermediary or this office for his/her business;
- ✓ an account which has been inactive for a long time all of a sudden becomes very active without there being a plausible explanation for this;
- ✓ they seem to be incompatible with the experience and knowledge the financial intermediary has of the client and the purpose of the business relationship.

2.2 As a rule, any client is suspicious who provides false or misleading information or who refuses to provide data and/or documents necessary for the business relationship and the relative activity without a plausible reason.

2.3 One reason for suspicion could be if a client regularly receives transfers from a bank domiciled in a country deemed to be high risk according to the Financial Action Task Force (FATF), or if a client repeatedly makes transfers to such a country.

2.4 Another suspicion could also be if a client repeatedly transfers funds to areas which are geographically close to operational areas of terrorist organizations.

II. Specific indicators

3. Spot transactions

3.1 Changing large amounts in bills (domestic or foreign currency) with small denominators to bills with large denominators;

3.2 Changing currency for a significant amount of money without recording it on a client account;

3.3 Cashing checks or traveler's checks for larger sums;

3.4 Purchase or sale of larger amounts in precious metals by walk-in clients;

3.5 Purchase of bank checks in a significant amount by walk-in clients;

3.6 Money transfers abroad by walk-in clients without a perceivably legitimate reason;

3.7 Repeated spot transactions in an amount just below the identification threshold;

3.8 Acquisition of bearer shares in physical form.

4. Bank accounts and depository accounts

4.1 Frequent cash withdrawals without there being a perceivable legitimate reason for this;

4.2 Use of financing instruments which may be customary in an international trade environment but which are incompatible with the known activities of this client;

4.3 Accounts with frequent movements despite the fact that these accounts normally are not used at all or very infrequently;

4.4 Client's business relationship structure which does not make economic sense (large number of accounts with the same bank, frequent transfer of funds between accounts, excessive liquidity, etc.);

4.5 Granting of security (collateral, sureties) by third-party entities which are not known to the bank and which do not have a recognizable close relationship to the client and where it is not clear for what the security is being provided;

4.6 Transfers to another bank without indicating the recipient of the funds;

4.7 Acceptance of money transfers from other banks without any indication of the account number of the beneficiaries or the order-giving contractual party;

4.8 Repeated transfers of large sums abroad with the instruction that the recipient should be paid this sum in cash;

4.9 Frequent transfers of large sums from and to countries known to produce illegal drugs;

4.10 Granting sureties or bank guarantees to secure loans among third parties that do not conform to market conditions;

4.11 Cash deposits by many different people into a single bank account;

4.12 Unexpected repayment of a non-performing loan without a credible explanation;

4.13 Use of bank accounts using pseudonyms or numbered accounts to settle commercial transactions related to trade, crafts or industry;

4.14 Withdrawal of assets shortly after they have been deposited in an account (transitory account).

5. Fiduciary transactions

5.1 Back-to-back loans without recognizable or legal purpose;

5.2 Holding equity interest in non-listed companies on behalf of others where the companies' activities are not perceivable for the financial intermediary.

6. Others

6.1 Client's attempt to avoid personal contact with the financial intermediary.

III. Indicators triggering heightened suspicion

- ✓ Client's request to close down accounts without a paper trail and to open up new accounts in their own name or that of relatives;
- ✓ Client's request for receipts for cash withdrawals or delivery of securities which were not actually made or where the assets in question were deposited in the same institution;
- ✓ Client's request to perform payments by indicating an incorrect ordering party;
- ✓ Client's request that certain payments not be made through the client's accounts but through the financial intermediary's nostro accounts or through "for diverse" accounts;
- ✓ Client's request to accept or show the granting of credit collateral which is economically not possible or to grant a credit on behalf of others by providing fictitious coverage;
- ✓ Legal proceedings against a financial intermediary's client due to criminal activities, corruption, misuse of public funds or qualified tax offense