CASL INVEST

AML/KYC POLICY OF CASL LLC

(the "COMPANY")

Last Revised: September 15, 2022

1. GENERAL PROVISIONS

1.1. It is the policy of the Company to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the financing of terrorist or criminal activities. We will comply with all applicable requirements and regulations. Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the proceeds appear to have derived from legitimate origins or constitute legitimate assets. The Company has zero-tolerance policy for money laundering activities. Our AML/CFT policies, procedures and internal controls are designed to ensure compliance with all applicable regulations and will be reviewed and updated on a regular basis to ensure appropriate policies, procedures and internal controls are in place to account for both changes in regulations and changes in our business.

1.2. This Internal Know Your Customer and Anti Money Laundering Policy (Internal KYC/AML Policy) is approved by the Company's Board of Directors (Board) or, in case there is no Board of Directors in the Company – by the Chief Executive Officer (CEO) and will be kept under regular review.

1.3. This policy is adopted by the Company, as of the date written above, to be executed and observed by it, its employees, affiliates and service providers. It aims to prevent the use of the Company's services by criminal entities for the purposes of money laundering, financing of terrorism, fraud, corruption, or any other criminal activity. Also, to counter money laundering, the company uses the services of an external service provider, that has implemented a sophisticated electronic customer verification system. Furthermore, the Company, under no circumstances, accepts cash from or pays cash to its customers. The Company reserves the right to suspend any transaction of its customer that may be considered illegal or, in the Company employees' opinion, may be related to money laundering.

1.4. The Company understands and accepts the fact that operations with Virtual Currencies are high-risk in accordance with the understanding of most international organizations in the field of AML/CTF (such as, FATF and Wolfsberg Group). In this regard, this policy is aimed at identifying, assessing and controlling ML/TF risks in order to secure Company's customers and make their investments into Virtual Currencies as convenient and safe as possible.

1.5. The Company shall comply with requirements set out in the following acts, rules, regulations and good practice guidelines (Regulating Acts):

- Saint Vincent and the Grenadines Anti-Money Laundering and Terrorist Financing Regulations, 2014;
- Saint Vincent and the Grenadines Anti-Terrorist Financing and Proliferation Act 2015;
- Saint Vincent and the Grenadines Anti-Money Laundering and Terrorist Financing (Amendment) Regulations 2017;
- Saint Vincent and the Grenadines Anti-Money Laundering and Terrorist Financing Code 2017;
- Saint Vincent and the Grenadines Anti-Terrorist Financing and Proliferation Amendment Act 2017;
- other documents as may be applicable from time to time.

1.6. The employees shall bear personal liability, as established by laws and regulations, for complying with the Regulating Acts.

1.7. Hereunder are the minimum standards set out by the Company which must be complied with, but not be limited to, that include:

- Establishing and performing internal controls and policies to mitigate related risks;
- Establishing and maintaining risk-based CDD, identification and verification procedures including KYC procedures;
- Establishing and performing risk-based approach to the assessment and management of ML and TF risks faced by the Company and customers;
- Providing ongoing transactions monitoring and suspicious transactions analysis and reporting internally and to the relevant authorities;

- Maintaining appropriate records;
- Providing AML/CFT training for and raising awareness among all relevant personnel.

2. RESPONSIBILITIES OF COMPANY'S EMPLOYEES

2.1. The Company's employees must be aware of and strictly abide by the provisions of this Internal KYC/AML Policy, as well as the requirements of all the Company's policies. The Company requires its employees to fully adhere to such documents in preventing the use of the Company's services for ML, TF and/or sanction evasion purposes.

2.2. This policy must be communicated to all of the Company's personnel. The Company employees must confirm that they reviewed this policy by putting a signature in a list maintained by the Company for these purposes or by signing a copy of this policy.

2.3. Each employee of the Company is expected to know the requirements of Regulating Acts, and it shall be the affirmative duty of such employee to carry out these responsibilities at all times in a manner that complies with the requirements of the relevant laws and regulations. Particularly, the Company's employees must study any amendments to laws and other regulations that are posted at applicable reliable source of information (e.g. Saint Vincent and the Grenadines Financial Intelligence Unit (SVGFIU) websites, FATF websites).

2.4. If an employee knows or suspects, or has reasonable grounds for knowing or suspecting, that a person is engaged in money laundering or terrorist financing, he or she shall make an internal report to the MLRO as soon as is reasonably practicable after the information or other matter comes to them.

2.5. Company's employees must undergo regular training aimed at familiarizing themselves with the latest versions of the Company's policies and amendments to the Regulating Acts. Completion of each of such trainings shall be confirmed in writing by each employee.

3. MLRO ROLE AND RESPONSIBILITIES

3.1. The Company has a designated Money Laundering Reporting Officer ("MLRO"). The MLRO has overall responsibility for the establishment and maintenance of the Company's AML/CTF program and underlying systems and controls and will report to the Board/the CEO.

3.2. The Company will ensure that the MLRO has the relevant experience and understanding of AML/CTF to carry out his/her duties. The Company will fully support and ensure the MLRO has resources available for his/her role and will provide ongoing support and development for the MLRO.

3.3. The duties of the MLRO will include, but are not limited to:

- monitoring our compliance with AML/CFT obligations;
- being a focal point for all activities within the Company relating to AML and CTF;
- receiving all internal suspicious activity reports and, where deemed applicable, reporting to relevant authorities on the same;
- establishing the basis on which a risk-based approach to the prevention of money laundering and terrorist financing is put into practice;
- overseeing communication and training for employees;
- advising the business on new products / processes from an AML perspective;
- overseeing product modifications to ensure they comply with AML/CFT obligations;
- supporting and co-ordinating senior management focus on managing the money laundering/terrorist financing risk in individual business areas; and
- ensuring that the Company keeps and maintains all of the required AML/CFT records.

3.4. At least annually the MLRO is required to produce reports for the Company's Board/ CEO, including, but not limited to, the following items:

- confirmation that adequate customer due diligence information is being collected and that ongoing monitoring is taking place;
- summary data relating to complex or unusual transactions;

- number of internal consents / Suspicious Activity Reports (SARs) received from staff members;
- number of SARs sent externally;
- information on status of staff training within the Company;
- confirmation that all business records have been properly stored and are retained according to regulatory requirements;
- changes in the law/operating environment which do or might impact the business;
- changes in the risk matrix affecting the business; and
- contacts with the regulator.

3.5. The Company's Board/CEO will consider the report and take any necessary action to remedy deficiencies identified in it, in a timely manner.

3.6. The MLRO will wish to bring to the attention of the Board/CEO areas where the operation of AML/CTF controls should be improved, and proposals for making appropriate improvements. The progress of any significant remedial programmes will also be reported to senior management.

3.7. The MLRO has the power to:

- monitor the activities of all Company's departments in AML/CTF matters;
- access current and/or archive versions of documents / customer data acquired during KYC, with the right to copy or otherwise distribute them, particularly for the purpose of reporting to the relevant authority or in other circumstances according to Regulating Acts.

Our MLRO is: Jack Grows

Email: j.grows@caslinvest.com

4. CUSTOMER IDENTIFICATION

4.1. The Company's customers are natural persons.

4.2. The customer shall pass the KYC procedure - identification and verification of new customers. In order to confirm the customer's identity, the customer must provide the following information:

- *Full name* - name requirement helps us match the name provided in the form by the customer and the name that is provided in KYC documents;
- *Date of birth* - date of birth requirement helps us to detect underage users;
- *Country of residence and principal residential address* - countries that the Company doesn't support are not on the list;
- *Date of birth*.

4.3. The KYC verification will be passed via our GetId partner, by uploading a proof of ID (color copy of a passport, or national ID, or international driving license). In certain cases verification of residence (utility bill, bank statement with transactions, bank reference letter no more than 3 months old) and source of funds verification will be required.

4.4. At this stage once both documents are uploaded and the liveness selfie, GetID passes:

- Document Integrity Check;
- Text recognition;
- Face Match Check;
- Identity Check;
- Global Sanctions, PEP, Watchlists, Blacklists and Prohibited Countries Check;
- Additional Check (e.g. document completeness, check if photos are screenshots, check duplicate accounts etc.);
- AML Screening: International Sanctions, PEPs, Watchlists and Adverse Media.

4.5. In order to verify the received ID information, the Company reserves the right to request additional information, such as a photo of the listed identification document holder along with the submitted document and any other verification methods.

4.6. Customer shall not establish business relations with and customer's transactions shall not be processed if:

- the customer does not provide documents and relevant information necessary for proper KYC and CDD, including any additional documents and information;
- based on documents or other information, the Company has a suspicion that ML or TF may occur. The MLRO must be immediately notified of the relevant suspicion in order to make a decision on further actions;
- the customer is a resident of a prohibited country.

4.7. In case of KYC verification success, the Company approves the transaction. However, if no documents are provided during KYC verification then the transaction is declined.

4.8. If a natural person is identified, the Company must, in case of doubt, also identify the beneficial owner of the natural person, i.e., the person controlling the activities of the person. The suspicion of the existence of an actual beneficial owner may arise, in particular, if, in applying the due diligence measures, the Company becomes aware that there is an urge to use a natural person for establishing a business relationship or making a transaction. In this case, the Company's services will be refused.

4.9. Identification of politically exposed persons (PEP):

4.9.1. Politically exposed person is defined as an individual who is entrusted with prominent public functions, other than as a middle-ranking or more junior official, including the Head of State, Head of Government, Minister, Deputy Minister of Assistance, Member of Parliament or Member of the legislative body similar to Parliament, a member of the governing body of the political party, a Supreme Court or Constitutional Court, member of court of audition; member, ambassador, charges d'affaires and senior officer of the armed forces, member of the board of directors and administrative or supervisory bodies of the state company, the head of an international organization, a deputy leader and a member of the governing body or an equivalent person who is not an officer of a middle-ranking and more junior level.

4.9.2. Family members of a PEP include:

- a spouse or a partner of that person;
- children of that person and their spouses or partners; and
- parents of that person.

4.9.3. Known close associates of a PEP include:

- an individual who is known to have joint beneficial ownership of a legal entity or legal arrangement, or any other close business relations, with a PEP; and
- an individual who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the benefit of a PEP.

4.9.4. Identification of politically exposed person is provided by the Company's partner GetID. In case a PEP (a family member of PEP, a known close associate of PEP) was identified the service will be refused.

4.10. Identification of a customer who is subject to international sanctions:

4.10.1. The subject of international sanctions is:
- state, certain territory, territorial unit, regime, organisation, association or group, which are subject to the measures provided for by an instrument imposing an international sanction;
- natural or legal person, institution, partnership or any other entity expressly mentioned in an instrument imposing or implementing an international sanction and to whom the measures provided for in the instrument imposing an international sanction are taken.

4.10.2. Identification of a customer who is subject to international sanctions conducted by the Company's partner GetID. In case such person was identified the service will be refused.

5. RISK ASSESSMENT

5.1. Based on the information gathered via the registration and KYC process, the Company shall assemble an individual profile of the customer upon entry into a business relationship (Customer Profile). The Customer Profile shall allow the Company to understand the customer's financial background, the origin of the assets involved into transactions, and the purpose of the business relationship, as well as to check their plausibility in terms of legitimacy, or to identify circumstances that require particular clarification. Based on the Customer Profile the Company shall perform a risk assessment, to determine the customer's Risk Profile and the necessary corresponding mitigating due diligence measures to be taken (Risk Profile).

5.2. The risk assessment shall take into account the following risk categories, the probability and consequences of their realization and the probability of an increase in the risk:

- geographical risks;
- customer-related risks;

- transaction-related risks;
- interface-associated risks.

5.3. Geographical risks, whose factors arise from differences in the legal environment of various countries, these factors may include situation when the customer is located in such jurisdiction:
  - countries identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective systems to counter money laundering or terrorist financing;
  - countries identified by credible sources as having significant levels of corruption or other criminal activity, such as terrorism, money laundering, and the production and supply of illicit drugs;
  - countries subject to sanctions, embargos or similar measures issued by, for example, the European Union or the United Nations;
  - countries providing funding or support for terrorism;
  - countries that have organizations operating within their territory which have been designated by Saint Vincent and the Grenadines, international organizations as terrorist organizations.

5.3.1. The usage of the Company is prohibited for the citizens of the following countries and territories:

- United States of America;
- Democratic People's Republic of Korea;
- Republic of Iraq;
- Republic of the Sudan.

5.3.2. The usage of the Company's services is prohibited, if a customer or a transaction are explicitly connected with the following countries or territories:
- any countries or territories under UN sanctions, and further under any embargo or similar measures, except Russian Federation;
- countries with insufficient measures for preventing money laundering and terrorism financing;
- countries, which according to reliable sources are involved in terrorism support, or countries with high corruption level, except Russian Federation.

5.4. Customer associated risks, whose factors arise from the person participating in a transaction. These factors may include:

- whether the customer is a PEP, family member of a PEP, or known close associate of a PEP;
- the residency of the customer, including whether the customer is registered in a low tax rate jurisdiction;
- whether the customer is included in international sanctions lists;
- circumstances (including those identified in the course of a prior business relationship) resulting from the experience of communicating with the customer, representatives and any other such persons;
- whether the origin of the customer's assets or the source and origin of the funds used for a transaction can be easily identified;
- the type and characteristics of the customer's business;
- the possibility of classifying the customer as a "typical customer"; and
- problems during the customer's identification procedures.

5.5. Transaction associated risks, whose factors result from the customer's activities or the exposure of a specific product or service to potential ML risks. These factors may include:

- the transaction involves substantial funds or unexplained source of funds;
- the transaction is part of series of suspicious transactions.

5.6. Interface associated risks, whose factors arise from the channels (mainly the Internet) through which the business relationship is established, and the transactions are carried out, these factors may include:

- whether the channel facilitates anonymity; and
- whether the channel facilitates third party funding.

6. TYPES OF RISK PROFILE

6.1. The conducted risk assessment shall result in a Risk Profile, identified through the risk factors mentioned in section 5 hereof, and according to the following scale:

6.1.1. Low Risk Profile

Customer is from the Recognized jurisdictions list. The latest approved version of the Recognized jurisdictions list, that is in Schedule 2 to the Anti-Money Laundering and Terrorist Financing Code of Practice, shall apply.
Low Risk Profile includes:

- usage of VPN or TOR browser in case if no other concerns are found;
- different IP with 1.8 proxy.

6.1.2. Medium Risk Profile

Customer is:

- not from the countries listed in low risk;
- there are one or more risk factors that differ from the sphere of the "typical" customer, but the transaction itself is clear (i.e. there are no risk factors in the transaction associated risks category). At the same time, there is no suspicions that a combination of the risk factors may indicate high risk of ML/TF.

Medium risk Profile includes:

- customer's date of birth ranges from year 1958 to 1968.

Depending on amount of risks, the customer may be called by the Company's representative to ask security questions if there are concerns.

6.1.3. High Risk Profile

Customer is:

- from a jurisdiction that, according to credible sources such as mutual evaluations, detailed evaluation reports or published follow-up reports, has not established effective AML/CFT systems;
- from a jurisdiction that, according to credible sources, has significant levels of corruption or other criminal activity;
- from a jurisdiction that is subject to sanctions, embargos or similar measures issued by, for example, the United Nations;

- from a jurisdiction that provides funding or support for terrorist activities, or that has designated terrorist organizations operating within their country, as identified by the United Nations;
- Customer Profile rises suspicions;
- there are multiple risk factors and the transaction itself is not clear. The combination of these factors cast doubt on the transparency of the customer's identity and transactions, indicating of ML/TF.

High risk Profile includes:

- customer's birth date 1957 and earlier;
- high risk IP identified by partners;
- different customers using same device/browser.

Proof of residence and proof of funds are mandatory for the customers under high risk category. The customers elderly of age above 65, that are considered high risk customers for scam and may require additional verification from the Company (video verification and/or phone call from one of our representatives).

Where the customer's Risk Profile is high in addition to the measures described above, the Company may consider obtaining further verification measures, which shall be approved by the Board/CEO. These may include:

- additional documents, data or information originating from a reliable and independent source;
- a notarized or officially authenticated copy of the identification documents.

6.1.4. Potential fraud category includes:

- Cardholder name differs from the name in uploaded documents;
- Phone number is VOIP;
- Document forgery identified;
- RAT - Remote access tool identified.

In case of potential fraud, the Company rejects the transaction and

blocks the customer from all future attempts.

6.2. If a potential or existing customer either refuses to provide the information described above when requested, or appears to have intentionally provided misleading information, we will refuse the services. In either case, our MLRO will be notified so that we can determine whether we should report the situation to the authorities.

6.3. If the Company identifies such activities or circumstances, the characteristics of which indicate the use of proceeds from a criminal activity, the financing of terrorism or the commission of related crimes, or an attempt of such activity, or if he is suspicious or knows that there is money laundering or terrorist financing or the commission of related crimes, MLRO immediately informs the FIU thereof, but no later than two working days after the establishment of the activity or circumstances or the suspicion of the occurrence of a suspicion.

6.4. The Company will monitor customers' activity for unusual size, volume, pattern or type of transactions, taking into account risk factors and red flags that are appropriate to our business. The MLRO or her designee will be responsible for this monitoring, will review any activity that our monitoring system detects, will determine whether any additional steps are required, will document when and how this monitoring is carried out, and will report suspicious activities to the appropriate authorities. The MLRO or his/her designee will conduct an appropriate investigation and review relevant information from internal or third-party sources before the authorities are notified. We monitor possible insufficient or suspicious information provided by the customer, particularly when the customer:

- Provides unusual or suspicious identification documents that cannot be readily verified;
- Reluctant to provide complete information about nature and purpose of transaction, anticipated account activity etc.;
- Refuses to identify a legitimate source for funds or information is false, misleading or substantially incorrect;
- Background is questionable or differs from expectations based on business activities.

6.5. The Company will perform AML checks within the following but not limited databases: EU sanctions (EU), United Nations sanctions

(UN). The Company will be monitoring customer transactions on a daily basis in real-time for risk within above-mentioned databases. Furthermore, all existing clients will be screened against the updated databases every day.

6.6. The Company customer support is available via online live chat / email, accessible on our site in case assistance is required. Support has access to confirm a transaction if successful verification was passed by GetID, has the rights to demand additional verification in case of high risk or reject a transaction. All processes and actions are made via our own secure CRM system and its admin panel. Our customer support can find a user by an e-mail address. No other data sensitive information is visible to our support members and we do not disclose personal information to any third party.

7. DATA COLLECTION AND STORAGE

7.1. The Company records the following data:

7.1.1. customer's data form;
7.1.2. date or term of the transaction;
7.1.3. description of nature of the transaction;
7.1.4. information regarding establishment of business relationships pursuant to customer's initiative or regarding the Company's refusal to establish business relationships;
7.1.5. information regarding termination of business relationships, including pursuant to inability to apply due diligence measures;
7.1.6. information regarding lending of virtual currency, amount of virtual currency, interest rate;
7.1.7. where opening a crypto currency wallet, its type, number (public key) and name of the relevant crypto currency.

7.2. The Company keeps the following documents for no less than five (5) years following termination of business relationships with the customer or his/her last transaction:
7.2.1. information and documents provided for identification of customer and verification of customer's data;
7.2.2. correspondence with the customer;
7.2.3. data collected in due course of monitoring business relationships;
7.2.4. data on suspicious and unusual transactions;
7.2.5. documents relating to transactions.

7.3. When collecting and storing data as well as customers' documents, the Company employees shall apply personal data protection measures. If a separate consent of the customer for processing of personal data for different aim had not been obtained, collected data may only be processed for the purposes of anti-money laundering and combating terrorism financing and provision of relevant service. Processing of data in a form which is not compliant with this aim is strictly prohibited.

8. IDENTIFICATION INFORMATION AND DOCUMENTS UPDATES

8.1. Customer's ID Information shall be updated:

- For Low Risk Profile customers once every 4 years;
- For Medium Risk Profile customers once every 4 years;
- For High Risk Profile customers once every 12 months.

8.2. In the event the customer does not provide the requested updated information, the provision of the Services must be suspended.

8.3. When the customer's transactions indicate significant changes in the Risk Profile, scope of activity or the amount of the customer's transactions, the information about the risk level of the customer shall be updated as soon as it becomes available.

8.4. The MLRO or specifically authorized employee shall perform routine sampling of the Customer Profile, reviewing the appropriateness and completeness of such Customer Profile and the processes documented therein. If the data used to identify the customer was not subject to verification within a reasonable period of time or there are reasonable grounds to suspect that the customer's account is inactive, the account may be canceled.

9. IDENTIFYING SUSPICIOUS TRANSACTIONS

9.1. The reviews described above shall aim at detecting:

- any discrepancies between the information previously gathered (as documented in the customer's Risk Profile) and any information which is currently known or is available to the Company (e.g. any updates or changes which have occurred in the customer's details);

- any discrepancies between the customer's Risk Profile and the transactions undertaken by it (e.g. transactions which do not seem to match the customer's financial status or expected scope of business); and
- any other suspicious behavior or pattern (e.g. transactions with no visible business logic, frequent purchase/sale of investments).

9.2. If any of the above is detected by an employee, or by any other means, it shall immediately be reported to the MLRO.

9.3. An employee does not need to have evidence that ML is taking place in order to have a suspicion of such ML. All employees will be encouraged to seek advice from their MLRO if they have any queries.

10. INTERNAL REPORTING

10.1. Internal reporting of any suspicious matters in connection with this Internal KYC/AML Policy shall be made immediately by the individual having such suspicions to the MLRO.

10.2. Any internal report should be considered by the MLRO, in the light of all other relevant information, to determine whether or not the information contained in the report does give rise to knowledge or suspicion, or reasonable grounds for knowledge or suspicion, of money laundering or terrorist financing.

10.3. The MLRO must be notified of any decline to establish a business relationship, suspicion of ML or unusual transactions, as well as cases of emergency cancellation.

10.4. The MLRO, upon receiving a report (or in any other manner becoming aware of any suspicion of ML/TF), shall immediately review such suspicion, evaluate its merits, and conclude what actions shall be taken in connection therewith. In doing so, the MLRO may consult the employee who reported the suspicion, the Board/CEO, or any other person within the Company.

10.5. The actions which the MLRO may decide to be taken may vary depending on the circumstances, and include any action mentioned in this Internal KYC/AML Policy. This includes, but is not limited to:

- no action;
- instructing the relevant employees to conduct further review;
- reclassification of the risk level of the customer;
- transactions limitation;
- immediate suspension or cancelation of the customer's account;
- reporting to the Board; and
- reporting to authorities, as further described below.

11. EXTERNAL REPORTING

11.1. If the MLRO concludes that the internal report does give rise to knowledge or suspicion of money laundering or terrorist financing, he must make a report to the FIU as soon as is practicable after he makes this determination. The MLRO's decision in this regard must be his own, and should not be subject to the direction or approval of other parties within the Company.

11.2. The FIU and the national reception point for disclosure of suspicions, and for seeking consent to continue to proceed with the transaction or activity, is Saint Vincent and the Grenadines Financial Intelligence Unit (SVGFIU). The SVGFIU address is P.O. Box 1826, Kingstown, St George, VC0100, St. Vincent and the Grenadines, and it can be contacted during office hours on: 1 (784) 451-2070. Urgent disclosures, i.e., those requiring consent, should be transmitted electronically over a previously agreed secure link.

11.3. The person about whom the FIU has been reported to shall not be informed in any manner.

11.4. Under the money laundering regulations, 'tipping off' is an offence. Once an internal or external suspicious activity report has been made, it is an offence for anyone to release information to any other person which is likely to prejudice a current or proposed law

enforcement investigation (in particular tipping off the actual person who is the subject of the suspicion).

11.5. Tipping off risks become real once a suspicious activity report has been made to the MLRO and where the MLRO agrees with the underlying suspicion and submits a report to the FIU. All communication between staff and the customer(s) from that point on needs to be handled with care, the MLRO will provide advice as to how to handle such situations.

12. INTERNAL CONTROL

12.1. The internal control procedures are a set of measures carried out by the Company to mitigate and manage effectively the risks of money laundering and terrorist financing identified in its risk assessment. Internal controls aim at maintaining the legality and efficiency of the Company's activities and must ensure compliance with the Regulating Acts, as well as collection of accurate, timely and reliable information, its handling and storage.

12.2. Internal control procedures cover all Company's activities, management team and their orders, business conduct and procedures, as well as the work culture in general, compliance with which should ensure the management of ML and TF risks. The Company must identify, analyse and document ML/FT risks and work towards reducing them.

12.3. The Board/the CEO has a responsibility to ensure that the firm's policies, controls and procedures are appropriately designed and implemented, and are effectively operated to reduce the risk of the firm being used in connection with money laundering or terrorist financing.

12.4. MLRO shall develop and the Board/the CEO should adopt the Company's internal policies and procedures, including this Internal KYC/AML Policy, aimed at assessing the degree of risks and countering ML and TF binding for all Company's employees, which should at all times cover the following matters:

- model risk management practices;
- KYC/CDD procedures;

- record-keeping;
- internal control and compliance management;
- suspicious transactions monitoring and reporting;
- corporate trainings.

12.5. The Board must verify that Company's internal policies and procedures, including this AML/KYC Policy, comply with current legislation and to task MLRO to amend them when necessary, or establish new policies and procedures.

12.6. The Board along with MLRO shall also oversee the implementation of this AML/KYC Policy and any other documents as may be applicable, with accordance to the AML/CTF requirements of the Regulating Acts.

12.7. The Board of the Company or a person(s) designated by it shall procure conducting of due diligence measures based on Regulating Acts and this policy, as well as procure that such measures are adequate and coherent with customer profile, nature and volume of the transaction and risks of money laundering and terrorism financing.

12.8. The Board of the Company procures that sufficient resources are allocated for performing of provisions of this policy and provisions of Regulating Acts and that the employees involved in procuring compliance with the relevant requirements are made fully aware of provisions of Regulating Acts and this policy.

12.9. In addition to any other duty under this AML/KYC Policy, the Company's Board/CEO shall be responsible for the following:

a) Risk Appetite: the total of the exposure level of ML/TF risk which the obliged entity is prepared to assume for the purpose of its economic activities and attainment of its strategic goals. The Board shall establish the total ML/TF risks exposure level and types that the Company is prepared to assume in pursuing its business objectives (Risk Appetite).

b) Annual compliance review: the Board shall convene on an annual basis to review and assess the effectiveness of this

AML/KYC Policy, the procedures taken under it, and the efficiency of the compliance function in general.

c) Supervision of Company's management positions with regard to AML/CTF: the Board shall be responsible to supervise the MLRO and other applicable office holders and shall have the authority and responsibility for their appointment, removal and replacement.

d) Has the right to approve high risk profile users account creation, business relationships and transactions.

12.10. At least once every four (4) years the Board shall assess the necessity for the Company to create an independent internal audit function or to hire an independent third party audit team in order to enhance its AML/TF measures by, among other, auditing the existing policies and rules. When making such an assessment the Company's management shall take into account the Company's size and size of its operations, prior history of suspected money-laundering among the Company's customers, regulatory obligations etc. The internal audit mechanism will evaluate and analyse the internal control system set out herein, its effectiveness and compliance with legal requirements and international standards. If necessary, a third-party specialist with appropriate qualifications will be recruited to conduct an internal audit, and as a result of such internal audit, the processes, operations, functions and actions of the Company will be assessed. Results of the internal audit should be reported to MLRO.

13. COOPERATION AND EXCHANGE OF INFORMATION

13.1. The Company cooperates with law enforcement agencies and other authorities in preventing money laundering and terrorist financing by replying to their requests for documents or information available to the Company in accordance with the applicable law.

13.2. The Company replies to a respective request sent at feedback@caslinvest.com, the MLRO's email or at the Company's registered address within ten (10) business days from the moment of its receipt if other deadline is not set by the applicable law.

13.3. The Company's MLRO is the employee responsible for processing any external requests within the Company. MLRO may seek necessary information from other functions in the Company in order to fulfill a specific request.

13.4. The Company ensures appropriate confidentiality while handling any requested information.

14. TRAININGS

14.1. Training and education of all relevant employees within the Company plays a critical role in the successful implementation of the risk based approach to managing potential ML/TF risks. All relevant employees must be aware of and understand the legal and regulatory environment in which they operate, including relevant ML prevention provisions, as well as the Company's own measures to give effect to the risk based approach.

14.2. Training the Company's employees for any requirements on preventing terrorism financing and money laundering shall be the responsibility of a management, or an employee authorized by the management, or a corresponding professional.

14.3. Management of the Company shall procure training of all relevant employees and agents (if applicable) who are responsible for establishing business relationships with customers and performing transaction whose work is relevant to the AML compliance of the practice or who otherwise contributes to identification or mitigation of the risks of ML/TF to which the Company's business is subject, and prevention or detection of ML/TF in relation to the Company's business. The training shall, among others, include information regarding employees' obligations under this policy (including procedures of identifying and reporting suspicious transactions, business relationships or activities), current money-laundering and terrorism financing techniques and related risks, measures for protection of personal data, measures for identification of potential money laundering or terrorism financing transactions, as well as guidance on steps that need to be taken in such cases, and the identity and responsibilities of the MLRO.

14.4. Employee trainings shall be carried out when needed, but in any event no less than once in a year, and details of any training shall be recorded.

14.5. All employees must be aware that non-compliance with this matter could result in disciplinary proceedings which could ultimately lead

to dismissal. Failure to comply with this policy could also result in legal action, including criminal action, being taken against them.

14.6. The employee confirms participation in the training with his/her signature.

14.7. MLRO is responsible for oversight of the Company’s compliance with its requirements in respect of staff training.