AML POLICY
PART I – INTRODUCTION

1. Preliminary statement
A policy counteracting money laundering and financing terrorist activities has been developed by Comax Invest Limited a company having its registered office at:Trust Company Complex, Ajeltake Road, Ajeltake Island, Majuro, MH96960,Marshall's Islands, registration number 103759; in order to carry out a battle with sponsorship of terrorism and money laundering, reduce financial and legal risks of the Company, implementation of appropriate measures aimed at preventing the risk of money laundering and terrorist financing. This document sets out the measures and plans, which will be implemented by us in respect of the aforementioned objective.

Implementation Guide

One of our objectives is to provide a secured system against money-laundering while ensuring that any clients who are potentially engaging in such activities will be exposed. Furthermore, we aim to make the entire trading process safer for our law-abiding clients and will do anything in our power to combat money-laundering. We are proud to state that we work in full cooperation with our client's local government and law enforcement agencies ensuring safe practices. That is why we have created a state-of-the-art security system that checks all customer credentials while storing in-depth logs of all of our transactions.

It is our duty to inform the authorities of any transactions that appear to be dubious. If you are not using our services for their stated purpose exclusively, you and any related parties could face legal ramifications.

In an effort to counter money laundering and other illegal activity, we have decided not to support any cash transactions, regardless of their stated purpose. Our firm has the right to cancel or deny a transaction at any point if there are suspicions regarding its legality. As stated in accordance with international law, the firm is under no obligation to notify the customer that it has contacted the appropriate legal authorities regarding a dubious transaction.

Policy of Compliance

We have created a policy of compliance for the purpose of meeting all lawful criteria regarding money-laundering. The policy refers to the election of officers in charge of compliance, creating new policies and making sure that they are properly implemented.

We constantly update our system, execute routine maintenance checks for any dubious transactions and verify all customer credentials while implementing any regulatory changes that might be necessary. Furthermore, our team has received the necessary training with regards to any and all measures with regards to countering money-laundering activity.

2. What is money laundering?

The phrase money-laundering refers to the act of moving money in various transactions in order to hide its source, its destination and who the original owner is. It is mostly done when the money has been obtained through unlawful means. Simply put, money launderers try to make money obtained illegally appear to be legal.
Money laundering is a crime, which is most often associated with banking and money transfer services. While banks are often the main part of successful laundering schemes, financial and other related services provided by different service providers, are also defenseless and can be used for money laundering.
Money laundering is sometimes incorrectly regarded as an activity, which is connected with organized crime or illegal drug trafficking. This is not true. It happens every time when any person has to deal with another person's direct or indirect benefit from a crime.
The term "money laundering" is actually a misnomer. Often it is not money, which is laundered but other forms of property, which directly or indirectly represent a benefit from a crime. Any form of tangible or intangible property can represent another person's benefit from a crime.
Traditionally, money laundering is described as a process that takes three stages:
Placement - This is the first step during which illegal funds are separated from their illegal source. Placement includes initial introduction of illegal funds into the financial system or transfer of cash across borders.
Layering - After the successful introduction of illicit funds into the financial system, their laundering requires to create multiple layers of transactions, which then separate the funds from their illegal source. The purpose of this step is to make it difficult to track the illegal source of these funds.
Integration - is the final stage of a complete money-laundering operation. It includes placement of illicit funds back into legal economy. The funds now represent net profit. Integration of funds should allow a criminal to use the funds so that no suspicion is aroused, which could lead to investigation or prosecution.
In fact, these three stages often overlap, and the benefits of many crimes, including the majority of financial crimes, should not be "placed" into the financial system.
Money laundering is a crime, which is most often associated with banking and money transfer services. While banks are often the main part of successful laundering schemes, financial and other related services provided by different service providers, are also defenseless and can be used for money laundering.
Thus our business is fully dedicated to obstructing any such acts of money-laundering and other related illegal matters.
3. What is terrorism financing?
Financing of terrorism is an act of economic support of acts of terror, terrorists or terrorist organizations to enable them to carry out terrorist acts. Unlike other criminal organizations, the main goal of terrorist groups is non-financial.

Nevertheless, like all organizations, terrorist groups need financial resources to perform basic operations. This simple fact, the need for funds, is the key in the fight against terrorism. Money tracking, following financial trail is the main purpose of all the measures, which are aimed to identify, trace and prevent financing of terrorism.
After the 11th September events in the United States, prevention of terrorist financing by the financial sector has gained equal status with as prevention of laundering of proceeds derived from criminal activity.
There are similarities and differences between money laundering and terrorist financing
Differences:
● Financing of terrorism is an activity that supports future unlawful acts, while money laundering generally occurs after commitment of unlawful acts.
● A legally obtained property is often used to support terrorism, whereas the origin of laundered funds is illegal.
Similarities:
● Terrorist groups are often involved in another form of criminal activity, which probably, further finances their actions.
● Both money laundering and terrorism financing require assistance of the financial sector. The key to prevention of money laundering and financing of terrorism is the adoption of appropriate measures to check Client Due Diligence (CDD) at the beginning of each relationship, as well as on an ongoing basis after that.

4. AML/CFT International Legislative Initiatives

The international community has taken and continues to take joint actions aimed against money laundering and terrorist financing. The company is aware of the most influential initiatives, which international financial centers must comply with.
Financial Action Task Force on Money Laundering (FATF) www.fatfgafi.org.
Forty recommendations and nine special recommendations of the FATF on terrorist financing are the most influential supranational initiatives in this area.
Caribbean Financial Action Task Force (CFATF) www.cfatf-gafic.org/
An organisation of states and territories of the Caribbean basin which have agreed to implement common counter-measures against money laundering. It is one of eight regional groups of the FATF.
Basel Committee on Banking Supervision www.bis.org
Although the name suggests that the Basel Committee is interested exclusively in the conduct of banking business, it brings an authoritative influence on formation of opinion about the importance of the effective check of the client due diligence throughout the financial sector. The act of the Basel Committee on CDD clearly demonstrates the importance of the CDD information in risk management.
Wolfsberg Group www.wolfsberg-principles.com
The Wolfsberg Group, which includes some of the world's leading private banks, has published global recommendations on combating money laundering and the Statement on the Suppression of the Financing of Terrorism.
International Organisation of Securities Commissions (IOSCO) www.iosco.org.
In 1992, the IOSCO adopted a resolution that encourages the IOSCO participants to consider issues relating to the minimization of money laundering. In May 2004, the IOSCO adopted the Act on Principles on Client Identification and Beneficial Ownership for the securities industry. The IOSCO Report on Principles sets out a comprehensive mechanism associated with the CDD requirements, which complements the FATF Recommendations and is aimed at taking the role of securities regulator in monitoring of the industry compliance with the AML obligations.
International Association of Insurance Supervisors (IAIS) www.iaisweb.org
The IAIS has given a high priority to the fight against money laundering and financing of terrorism. In October 2003, the IAIS revised and expanded its basic principles and insurance methodology. Compliance with these basic principles is necessary for the effective supervisory system of insurance. As part of this review, a new basic principle 28 was introduced, which specifically treats the issues of the fight against money laundering and terrorist financing. In October 2004, the IAIS adopted a new guideline for combating money laundering and terrorist financing. This methodological development has replaced the methodological development on combating money laundering, which was published in January 2002 for the authorities supervising the activities of insurance companies and insurance organizations. This new guideline has incorporated the revised FATF 40 + 8 special recommendations and recommendation compliance assessment methodology into the FATF 40 + 8 Special Recommendations published in February 2004.

4. Additional territorial authority of the United States

After the events of 11 September, the United States has promptly introduced a new part of legislation, which is called the USA PATRIOT Act. This legislation has further expanded the territorial civil and criminal jurisdiction of the United States, making changes in the existing US legislation to combat money laundering. Now the courts of the United States can claim jurisdiction over any foreign person, including any financial institution authorized in accordance with legislation of a foreign country, if a person commits any offense according to the US law on combating money laundering. This means that any foreign person conducting a transaction using the US dollars is exposed to the jurisdiction of the US courts against the US crimes related to combating money laundering.

5. Legal Framework in Marshall Islands

The main legislative act on anti-money laundering and counter-terrorism is:
Anti-Money Laundering Regulations, 2002

PART II – GLOSSARY AND CONTENTS

1. Interpretation In this document, unless the context otherwise requires,
the Law is the law on prevention of laundering of proceeds derived from criminal activities in 2001.
AML/CFT denotes the fight against money laundering and opposition to terrorist financing.
AML/CFT program is a program developed for implementation of an anti-money laundering and counter terrorist financing policy in accordance with the current normative legal documents and international standards on countering legalization (laundering) of proceeds from crime and terrorist financing.
AML/CFT requirements are requirements described in Part III.
Beneficial owner is a person who:
a) has effective control over a client or a person on behalf of whom the transaction is carried out; or
b) owns a prescribed threshold of a client or a person on whose behalf a transaction is being conducted
Business relations are business, professional or commercial relations between an affiliated company and a client, which are long-continued or which at the time of establishment of contact are considered by the affiliate as long-long continued
Cash money:
a) physical currency
b) negotiable instrument of a bearer
Company: is Comax Invest Limited
Client:
a) is a new client or an existing client; and

b) includes: (1) instrument holder; (2) a person conducting or seeking to conduct a single transaction with the Company. Instrument is any account or agreement provided by the Company and through which the instrument holder can carry out 2 or more transactions.

Financial institution:

a) a person who, during an ordinary course of business activities, carries out 1 or more of the following financial arrangements:
(1) acceptance of deposits or other reimbursable funds from the public;
(2) a loan to a client or for a client, including a consumer credit, mortgage credit, factoring (with or without a turnover), and financing of commercial transactions (including forfeiting);
(3) financial lease (excluding finance leasing arrangements in relation to consumer products);
(4) transfer of money or value for or on behalf of a client
(5) release or management of payment means (e.g., credit or debit cards, receipts, traveler's checks, money transfers or electronic money);
(6) acceptance of financial guarantees and commitments;
(7) trading on a person's own account or at clients' cost in any of the following: (A) money market instruments (e.g., cheques, bills, certificates of deposit, or derivatives); (B) foreign currency; (C) exchange, interest rate and index instruments; (D) negotiable securities; (E) commodity futures trading;
(8) participation in securities issues and provision of financial services related to such issues;
(9) management of individual or collective portfolios;
(10) secure storage or management of cash, or marketable securities on behalf of others;
(11) investment, arrangement or management of funds or money on behalf of others;
(12) issuance or acceptance of obligations under a life insurance policy as an insurer;
(13) exchange of money and currencies;
b) includes a person or class of individuals who, according to a regulation, are financial institutions under Law; but
c) exclude a person or a class of individuals, who, according to a regulation, are not financial institutions under Law.

Financing of terrorism - is provision or collection of funds, or provision of financial services with understanding that they are intended to finance the organization, preparation or commission of terrorist crimes, or to finance an organized group, an illegal armed group.

Money laundering crime - is transformation of money or other monetary instruments gained from illegal activity into money or investments, which seem like legitimate so that their illegal source cannot be identified.

Single transaction

a) is a cash transaction that occur outside of business relationships and exceeds an applicable threshold value (regardless of whether the transaction is carried out by a single operation or several operations carried out, which appear to be linked); and
b) includes a transaction or a class of transactions which, in accordance with regulations, are single transactions; but
c) excludes (1) check deposits; and (2) a transaction or class of transactions that, in accordance with regulations, are not single transactions according to Law

Physical currency is a coin and printed money, which (a) is legal means of payment; and (b) are in turnover as, and are normally used and accepted as means of exchange in a country of issuance.

Politically exposed person is:

a) a person who holds or has held at any time in the last 12 months, in any foreign countries, a prominent public office:
(1) The head of a nation or head of a state, or a government; or
(2) Minister of State or equivalent senior politician; or
(3) Member of the Supreme Court or equivalent senior judge; or
(4) the head of the central bank or any other position that has a comparable influence, or;
(5) senior foreign representative, ambassador or high commissioner; or
(6) a senior member of armed forces; or
(7) a board chairman, manager or a chief financial officer, or any other position, having a comparable influence in any government enterprise; and
b) an immediate family member of a person referred to in paragraph (a), including
(1) a spouse; or
(2) a partner, whom the corresponding state law considers as equivalent to a spouse; or
(3) a child and a spouse or a child's partner; or
(4) a parent; and
c) taking into account information that is public or easily accessible,
(1) any person who is known to have a joint beneficial ownership right of a legal entity or legal arrangement, or any other close relationship with a person referred to in paragraph (a); or
(2) any person who has an exclusive beneficial ownership right of a legal entity or legal arrangement, which is known to exist in favor of a person described in paragraph (a)

Reporting entity

a) is (1) a financial institution; and (2) casino; and
b) it includes (1) a person or a class of individuals, who, according to regulatory provisions, are the object of a primary financial monitoring; and (2) any other person who, according any resolution, is obliged to execute the law, as if it were the subject of a primary financial monitoring; but
c) a person or a class of individuals, who, according to regulatory provisions, are not objects of a primary financial monitoring

Senior manager (and senior management respectively) is,

a) with respect to the object of a primary financial monitoring, which is a company director; and
b) with respect to the object of a primary financial monitoring, which is not a company, a person who occupies the position comparable to the position of a Director (e.g., trustee or partner); and
c) any other person, who occupies a position within the object of a primary financial monitoring, which allows such person to influence the management or administration.

Shell bank is a corporation, which (a) is registered in a foreign country and is authorized to conduct banking activities in the country of its registration, but has no physical presence in the country of registration; and (b) which is not a subsidiary of another corporation, which is registered in a particular country and authorized to conduct banking business in the country of registration; and which is sufficiently controlled and verified with regard to conduct of banking business; and has a physical presence in the country of registration.

Shady transaction is a transaction, which:

a) gives rise to a reasonable suspicion that it may involve money laundering or proceeds of crime; or means connected with or related, or used for terrorism, or acts of terrorism, or illegal organizations, regardless of whether the funds are the proceeds of crime or not;
b) performed in circumstances of unusual or unjustified complexity;
c) seems to have no economic justification or lawful purpose;

d) performed by a person or on behalf of a person whose personality has not been identified to satisfaction of a person with whom the transaction has been carried out; or
e) gives rise to suspicion for any other reason.

Transaction

a) is any deposit, withdrawal, exchange or transfer of funds (in any currency), carried out by (1) cash; or (2) by cheques, money order or other instrument; or (3) by electronic or other nonphysical means; and
b) without limiting the paragraph (a), includes (1) any payment performed, in whole or partially as a payment for of any contractual or other legal obligation; and (2) a transaction or a class of transactions, which are defined as transactions according to Law.
2. Application
The company is aware that the law is applied only to the extent that (a) financial activities undertaken by the Company are within the scope of actions described in the definition of financial institutions; or (b) the company carries out actions that may give rise to the risk of money laundering or terrorist financing.

PART III – REQUIREMENTS AND ADHERING TO AML/CFT

1. Due Diligence Measures for Clients (CDD)

1.1. When establishing a business relationship with a claimant upon business and on an ongoing basis, the Company will apply the appropriate CDD measures in the business relationship, including identification and verification of the applicant's identity for business.
1.2. The Company will carry out the CDD for:
a) a client;
b) a client's beneficial owner;
c) any person acting on behalf of a client.
1.3. A client who is a private person, and whom the Company reasonably trusts that he/she does not act on behalf of another person, shall be treated as if he or she is a beneficial owner, if the Company does not have reasonable grounds to suspect that the client is not a beneficial owner.
1.4. According to a quality risk profile, the Company executes a standard CDD, simplified CDD and a more severe CDD depending on the circumstances described in Part IV of this document.

2. Basis for verification

The Company shall carry out verification:
a) on the basis of documents, database, or information issued by a reliable and independent source; or
b) on any other basis relating to the indicated situation, client, product, service, business relationship or transaction as may from time to time be prescribed by Law.

3. Individuals

3.1. The Company will collect the relevant identification data about an individual, including:
a) a person's full name;
b) place and date of birth of a person;
c) current address of a person's residence (P.O. box address will not be accepted);
d) nationality;
e) any occupation, social position occupied and employer's name if available.
3.1.1. Individual identity verification:
The Company recognizes and guarantees that all collected identification details must be checked.
Identification documents will be received and kept to verify information provided by managers about their personality. The documents must be either original or properly certified, and must contain a photo of a manager.
When identifying a personality of an individual, the Company shall rely on the following types of documentation:
● internal identity documents;
● currently valid passports;
● currently valid driver's license.
3.1.2. Individual's address verification:
When verifying an individual's address, the Company may rely on the following types of documentation:
● a recent utility bill;
● a recent bank statement or credit card statement;
● recent bank references.
The term "recent" stands for the past three (3) months.
Alternatively, verification may be carried out by:
● receipt of a recommendation from a professional person who knows an individual (the recommendation must include the person's permanent address of residence);
● current list of electors checks;
● use of address verification service; or
● a person's visits of his/her current address of residence.

4. Person other than an individual

4.1. Legal entities include corporate bodies, partnerships, associations or any other entity except for legal agreements.
4.2. When an applicant for business is a legal entity, the Company:
a) ensures that it understands the structure of ownership and control of the applicant for business; b) check and verify the existence of a legal entity and
c) will determine the identity of a legal entity managers.
4.3. For the purposes of paragraph 4.2 above, managers of applicants for business include the following persons:
a) organizers;
b) beneficial and final beneficial owners;
c) officials;
d) inspectors;
e) company's directors.
4.4. The Company shall:
a) identify and verify the identity of a legal person, including the name, date of registration, date and country of registration or entry in register;
b) identify and verify registered office address and principal place of business (if it differs from registration office);
c) check a legal person's legal status;

d) identify and verify principal managers' identity (including beneficial owners, supervisors, director or equivalent position) having ultimate effective control over capital or a legal entity's assets; and
e) check that any person who intends to act on behalf of a legal entity, has an appropriate permission for that, and identify that person.
4.5. If the principal managers are not natural persons, the Company shall establish the identity of individuals who ultimately own or control the business and check their identity in accordance with the requirements set out in this document in general in relation to to natural persons.
4.6. Identification and verification requirements applicable to legal entities may be fulfilled in various ways depending on applicant's nature, i.e. in respect of private companies, trusts and partnerships:
4.6.1. Private companies:
● obtainment of original or duly certified copy of a company's incorporation certificate or entry in register;
● verification of corresponding registration of companies, that a company continues to exist;
● reviewing of the latest report copy and accounts if available (audited, where applicable);
● obtainment of details about the registered office and place of business;
● verification of identity of the company's executives as mentioned previously.
4.6.2. Partnership:
● receipt of original or a duly certified copy of a partnership agreement;
● if a partnership has been registered, verification of the relevant registration that the partnership continues to exist;
● receipt of the latest report copy and accounts;
● confirmation of a partnership business nature in order to ensure its legality;
● verification of executives' identity as mentioned previously.
4.6.3. Trusts:
a) Trusts do not have a separate legal entity, and therefore business relationships are formed through their business. A trustee of a Trust enters into a business relationship on behalf of the Trust and should be considered as the client along with the Trust.
b) When a Trust is an applicant for business, the Company shall
(1) ensure that it understands the structure of ownership and control of the claimant upon business;
(2) check and establish the existence of the Trust, and
(3) determine the identity of the Trust's executives.
In the context of this paragraph, the executives include:
● capital founders and participants;
● trustees;
● beneficiaries;
● defensors.
c) When identifying and verifying a Trust, the Company shall:
● receive original or a duly certified copy of a trust agreement or the relevant extracts from the agreement;
● if a Trust is entered into a register - check the relevant register to ensure that the Trust does exist;
● obtain the details of the legal office and place of business of a Trust;
● verify executives' identity of a Trust as mentioned previously.

If a claimant upon business is a company, a Trust, a partnership or any other organization, the Company will always verify the identity of the final executives-individuals of such candidates in the same way as the identity of clients who are natural persons.

5. Source of funds

The Company is aware that when identifying a risk and preventing money laundering, it is necessary to understand the origin or source of funds or property of the underlying business relationship with a client. Understanding of a source of funds/property of a client and a source of wealth of clients is an important aspect of the CDD.
A "source of funds" is an activity or a transaction that generates money for a client, while a "source of wealth" refers to actions that produced a total equity capital of a client.
Taking this into consideration, the Company will take appropriate measures to establish the source of income of each business applicant, and in case of involvement of a third-party funding – it will conduct further investigations with respect to relationship between a person providing funds and an applicant.
The company further ensures consistency between information available about an applicant for business and nature of (proposed) transactions.
If there is any sign of misleading or potentially suspicious activity within the context of provided product or service, the Company will take further action to verify the acquired information. In such a case, the Company will also consider information about obtaining information on the source of wealth of an applicant or client, which is one of the more advanced CDD measures applied in case of high risk.

6. Appropriate assurances

If the Company must rely on verification of non-original identity documents, they must be duly certified as true copies of original documents.
In the case of a private meeting of an applicant for business or its directors with the Company, an employee (or a Secretary or any other Company official) of the Company shall require the latter to provide the original documents, make copies of these documents and certify them personally as authentic copies of original documents. In other cases, the copies of documents can be certified by a lawyer, a notary, registrar, accountant or any other person having a recognized professional qualification, a director or a secretary of a regulated financial institution in EU or in an equivalent jurisdiction, a member of the judicial authority or a senior public servant.
A certifier must sign a copy of the document and clearly mark their name on it, their address and position or powers, along with contact information in order to help certifier tracking.
The company will take proper precautions, considering certified copies of documents, especially when such documents are issued by a country, which is at high risk, or by a non-regulated company in any jurisdiction.
If certified copies of documents are accepted, the Company is obliged to ensure compliance of a certifier. The Company shall further ensure that a client's signature on an identification document corresponds to the signature on application form or any other document.

7. Legal representative and group representative.

7.1. Given the fact that some clients may be presented by third parties/intermediaries to the Company, the Company may find it necessary to rely on the representatives in relation to the question concerning undertaking an obligation of conducting the CDD measures as it is specified in detail in the previous section. In order to avoid misinterpretation, we would like to specify that:
a) legal representatives are individuals or companies, which transmit business to the Company, and (1) regulated in matters of money laundering or (2) submit to the rules of professional conduct that are related to money laundering, and (3), is situated in a jurisdiction having legislation to combat money laundering, which is at least equivalent to the current one in EU;
b) A group representative is an organization, which is a part of the same group as the Company, and, for the purposes of combating money laundering, it is the subject of a consolidated supervision regulator.
7.2. The company can rely on representatives in respect of undertaking obligations to commit the following CDD measures:

a) identify and verify the identity of an for business using reliable, independent initial documents, data and information;
b) identification and confirmation of a beneficial owner in a way that would satisfy the Company and allow it to know who is the beneficial owner; and
c) obtainment of information about purposes and intended nature of business relationship Notwithstanding the aforementioned, the Company recognizes that if it relies on a legal representative or a group representative, the ultimate responsibility to ensure satisfactory acceptance of the CDD measures rests with the Company.
7.3. The Company can rely on representatives on issues of undertaking responsibilities to conduct the following CDD measures, provided that the following conditions are met:
a) procedures applied by legal representatives or group representatives, quite severe to ensure that the CDD measures are carried out in accordance with laws and regulations;
b) The Company has evidence on status of legal representatives or group representatives in the form of a Declaration, completed in accordance with sample attached in Annex 1;
c) The Company and legal representatives or group representatives have formalized their respective responsibilities in written form;
d) The Company itself was verified that legal representatives or group representatives have copies of identification data and other relevant documentation relating to CDD requirements and timely access to CDD information kept by legal representatives or group representatives, on request without a delay;
e) agreements entered into between the Company and legal representatives or group representatives include certain provisions relating to obligations under which legal representatives or group representatives will take all necessary CDD measures, and provide access to CDD information, and will send copies of the documentation of the Company CDD on request without a delay;
f) all document copies provided to the Company by legal representatives or group representatives must be properly certified.
7.4. If a representative of the Company ceases to act as such, the Company will have access to all CDD documentation, collected and stored by them during conducting CDD measures.
7.5. The Company will take their own CDD measures if they have doubts concerning a representative's ability to take appropriate CDD measures.

8. Imposing obligations on another affiliate or individual in another country

8.1. The Company can rely on another person (who is not an agent) on issue related to carrying out of proper CDD procedures, provided that:
a) a person on whom the Company relies, is a resident of a country with sufficient existing systems and AML / CFT measures and is controlled or regulated for the purposes of AML / CFT;
b) a person has business relationship with an interested client;
c) a person has carried out appropriate CDD procedures, at least, standard required by law and provided to the Company:
(1) relevant information on confirmation of identity before establishing business relationship or conducting a one-time deal; and
(2) relevant information about verification as soon as possible, but no later than 5 business days after establishing business relationship or executing a single transaction;
d) a person agrees to conduct CDD procedures for the Company and the Company's provision of the whole relevant information.
8.2. The Company recognizes that in spite of all the above described information in paragraph
8.1, it is the Company and not a third party, which is relied on, is responsible for ensuring compliance Laws and regulations.

9. Selection of time for verification of identity

The Company recognizes that it should complete all CDD measures for all applicants for business before establishing new relationships with clients and prior to providing any financial services.
If it is necessary, to provide services to an applicant for business before completion of CDD measures, a decision on similar provision will be properly taken by senior management and the reason for this decision will be formalized in written form.
The Company has to complete CDD measures as soon as reasonably possible, in any case so as to prevent interruption of normal course of business and to ensure effective management of money laundering risk.
The Company may delay the process of identity verification in the following situations, if it does not interrupt the normal course of affairs:
● indirect business;
● transactions in relation to securities (in securities industry, companies and intermediaries may be required a very rapid execution of transactions, according to the current state of market at the time when a client is reviewing them, and execution of a transaction may be required before identity verification is completed).
At risk management, the Company will make sure that:
● a transaction does not refer to relationships having high risk;
● identity verification will be completed as soon as it is practicable;
● funds received are not transferred to third parties;
● a number, types and/amount of transactions that can be carried out, have been limited; and
● the Company will control large and complex transactions.
If satisfactory CDD documentation is not received, the Company will be released from or terminate such business relationship and consider making a suspicious transaction report. The Company is aware of potential risks when entering into any form of relationship with any claimant upon business before taking CDD measures, which are satisfactorily completed. If the Company is unable to perform CDD requirements for an applicant for business, it will consider drawing up a report on a suspicious transaction for Commissioner.

10. Prohibition

10.1. In cases when CDD is not carried out, the Company:
a) will not establish business relationship with a client;
b) will end any existing business relationship with a client;
c) may not perform a single transaction with or for a client;
d) consider the possibility of drawing up a report on suspicious transactions;
e) can open the possibility of drawing up a report on suspicious transactions only to a person specified in the section "Disclosure of information related to reports on suspicious transactions".
10.2. In cases of false client names and client anonymity, the Company will not, deliberately or out of negligence, create an object of material support for a client on the basis of client anonymity without legal evidence or reasonable excuse, or under a client's false name. This, however, does not refer to objects of material support, (a) which have a number or other identifier assigned to them, and a client and any person who is authorized to act on behalf of a client in respect of that service, have gone through an identification process in accordance with CDD requirements; or (b) which have been created for an authorized body on regulation and control for law enforcement purposes.
10.3. The Company shall not establish or continue a business relationship or allow a one-time transaction, which will be carried out through it by a shell bank; or a financial institution that has corresponding banking relationship with shell banks.

11. Existing clients

In view of the fact that the threat of money laundering appears not only from applicants' for business side, but also from existing clients, the Company will, from time to time, assess the risk of their own client base, as well as the nature and extent of CDD information contained therein, or any additional documentation or information that can be requested for existing clients.
CDD requirements concerning the existing clients will be applied based on relevance and risks and CDD check will be conducted for the existing relations, if necessary, in situations including but not limited to the following:
● a transaction of a significant volume is carried out;
● user documentation standards change substantially;
● there is a significant change in a way an account/means is opened and maintained;
● The company is aware that there is lack of CDD information on an existing client.

12. Nonobservance

The Company recognizes and understands that:
1) The Law is inforce despite any contrary provisions in the contract or agreement.
2) No individual is not exempt from compliance with any requirements of Laws or regulations due to the fact that compliance with these requirements would lead to contract or agreement breach.

PART IV – RELATIONS WITH HIGH AND LOW RISK

1. Profiling/Risk assessment

After collecting CDD documents, the Company will perform initial assessment of risks to which the Company is subject by business relationships, and will assess a client accordingly. At this, the Company will take into account many factors including but not limited to the following:
● nature and type of a client;
● commercial rationale for relations;
● geographical location of a client's place of residence;
● geographical location of business groups and/or assets of a client;
● nature and value of assets involved in a relationship;
● source of a client's funds and, if necessary, a source of wealth;
● a role of any representative and regulated or professional status of a representative
The Company understands that, while risk assessment should be performed prior to entry into business relations, for some clients, a comprehensive risk profiling may become apparent only when a client has started to conduct transactions via the account/instrument. Therefore, the Company will carry out daily monitoring of client transactions and constant review, which are fundamental components of an appropriate risk assessment.
If the Company has estimated that business relationship or a single transaction are related to a relationship having a high risk, based on individual status of a client's risk, i.e. client's nature, business relationships, its location or any other characteristic aspects of business relationship, the Company will apply strict CDD measures as described further in this document, in Part IV.
Level of risk will be assessed in written form and identify the risks with which the Company will face in the course of its business; describe, as the Company guarantees, that assessment remains valid, and allow to determine risk level relative to its obligations under Law.

2. Review and audit of risk assessment and AML / CFT program

The Company will review its risk level assessment and AML/CFT program in order to to ensure that it remains effective, identify any defects and, if necessary, make any changes to fix these defects.
The Company will conduct an audit of risk assessment and AML/CFT program once a year or at any other time at the request of its AML/CFT external observer ensuring that audit is conducted by an independent person who has an appropriate qualification to conduct such audit.
A person appointed to this position may not be an accountant-expert or be qualified to conduct financial audits. Internal auditor should be independent and should not be involved in the establishment, implementation or maintenance of AML/CFT program of the Company and in the implementation of the Company's assessment of a risk degree.
The Company will provide a copy of any audit to their AML/CFT observer at request.

3. Annual AML/CFT report

The Company will prepare an annual report on their assessment of a risk degree and AML/CFT program, which will take into account the results and significance of the audit and contain any information prescribed by Law. Then the report will be provided to the AML/CFT external observer of the Company in accordance with and at request of the latter.

4. Applying AML / CFT requirements to offices and branches

The Company ensures that its foreign branches and subsidiaries apply measures broadly equivalent to those set out in Law, taking into account CDD requirements (including the ongoing CDD), risk assessment, AML/CFT programs and records storage to the extent expressly permitted by legislation of a country.
If a foreign country law does not permit application of such equivalent measures by offices or branches located in that country, the Company will consequently report to its AML/CFT observer and will take additional measures to handle effectively the risk of money laundering and terrorist financing.
The Company will report (where appropriate) its offices and branches, which are located outside registration country, about the policy, procedures and control means that it establishes, implements and supports, in accordance with this section.

5. Standard CDD

5.1. Application

The Company carries out standard CDD in the following cases:
a) if it establishes new relationship with a new client;
b) if a client is trying to carry out an occasional transaction with the Company;
c) if in relation to an existing client and according to a risk level, (1) there has been a significant change in the nature or purpose of a business relationship; and (2) the Company believes that it is lacking information about a client;
d) any other circumstances that may from time to time be determined by Law.

5.2. Identification requirements according to CDD

5.2.1. If an applicant for business is an individual, the Company identifies his/her identity in accordance with the arrangements set out in the general terms below:
a) takes reasonable steps to ensure that information on identity provided in accordance with Part III, is correct;
b) according to risk level, check the identity of any beneficial owner in order to know who this beneficial owner is;
c) if a person is acting on behalf of a client, according to a level of risk, it takes reasonable steps to verify the identity of a person and his/her authority to act on behalf of a client so that the Company knows who this person is and that this person has the authority to act on behalf of a client; and
d) checks any other information prescribed by Law

5.2.2. Except for information set forth in section
5.2.3 below, the Company will perform identification before establishing a business relationship or carry out an occasional transaction.
5.2.3. The Company may carry out identity checks after a business relationship has been established, if:
a) it is important not to interrupt normal business practices;
b) the risks of money laundering and terrorist financing are effectively managed through procedures of operating limitations and account control; and
c) identity verification is carried out as soon as possible immediately after a contract conclusion.

5.3. Other requirements

The Company shall also obtain:
a) information about the nature and purposes of a proposed business relationship between a client and a Company; and
b) sufficient information in order to define whether a client has to undergo a stiffened CDD.

6. Simplified CDD

6.2. Application

6.2.1. The Company may conduct a simplified CDD, if:
a) it establishes business relationships with one of the clients described in subsection (2) below; or
b) one of the clients, defined by the legislation carries out a single transaction with the Company; or
c) a client conducts a transaction or provides a product or a service as defined by Law, through the Company.

6.3. Identification requirements

The Company shall receive the following information on a person's identity acting on behalf of a client:
a) a person's full name;
b) a person's date of birth;
c) relationship between a person and a client; and
d) any other information, defined from time to time by legislation.

6.4. Identification requirements check

6.4.1. The Company, according to a level of risk, has to check the identity of a person acting on behalf of a client, and availability of a person's authority to represent the interests of a client so that it will know who this person is and that this person has the authority to act on behalf of a client.
6.4.2. Identity verification must be performed by the Company prior to establishing a business relationship or carrying out a single transaction, or the implementation of actions by a person on behalf of a client.
6.5. Other requirements In the situation described in paragraph 3.1 (2), the Company will also receive information about the nature and purposes of a proposed business relationship between a client and the Company.

7. Stiffened CDD

7.1. Application

7.1.1. The Company shall carry out a stiffened CDD in the following circumstances:
a) if the Company establishes a business relationship with a client who is (1) a Trust or other mechanism to hold personal assets; (2) a client belongs to a country that has inadequate systems and measures to combat money laundering and counter financing of terrorism; (3) a company with nominee shareholders or shares in bearer form;
b) if a client is striving to conduct an occasional transaction with the Company, and a client is (1) a Trust or other mechanism to hold personal assets; (2) a client belongs to a country that has inadequate systems and measures to combat money laundering and counter financing of terrorism; (3) a company with nominee shareholders or shares in bearer form;
c) if a client is trying to conduct a complex, an unusually large transaction or unusual transaction system through the Company, that have no apparent or visible economic or legitimate purpose.
d) when the Company believes that a risk level is such that a stiffened CDD should be applied to a particular situation;
e) any other circumstances prescribed by Law.
7.1.2. The Company shall carry out a stiffened CDD if:
a) it establishes a business relationship with a client, who is defined as a prominent political figure; or
b) a client, who is defined as a prominent political figure, tends to conduct an occasional transaction with the Company.
7.1.3. The Company will carry out a stiffened CDD if:
a) it establishes a business relationship with a client, which include new or developing technologies, or new or developing products that might be favourable for anonymity, or
b) a client is striving to conduct an occasional transaction through the Company using new or developing technologies, or new or developing products that might be favourable for anonymity.

7.2. Identification requirements

The Company understands that a stiffened CDD involves taking additional steps in relation to identification and verification. Such steps, according to a particular situation, may include, but are not limited to, the following:
● obtainment of more detailed CDD information from a client or from independent sources (such as Internet, public sphere or commercially available databases);
● confirmation of additional aspects of information received on CDD;
● obtainment of additional information requested in order to understand the purpose and intended nature of such business relationship;
● adoption of appropriate and reasonable measures to establish the source of funds and the source of a client's wealth, of any beneficial owner and the main executive;
● implementation of a more frequent and extensive control over such existing business relationships with the establishment of lower control thresholds for transactions related to such business relationships.

7.3. Politically Exposed Persons (PEP)

The Company will apply stiffened CDD measures, if she decides to enter into and maintain a business relationship with a PEP. It is connected with the fact that the nature of parties involved in scandals with the participation of PEPs attracts international media attention. Consequently, they can have an extremely negative impact on the reputation of the Company and in particular to the jurisdiction as a whole.
The Company will require the relevant information from an applicant, as well as to apply to publicly available information to determine whether an applicant or its beneficial owner is a prominent political figure, a family member or a close associate of such figure.
Usually, as soon as it is possible immediately after the establishment of a business relationship or carrying out a single transaction, the Company will take reasonable steps to determine whether a client or a beneficial owner is a political figure.
If the Company has determined that a client or a beneficial owner is a prominent political figure, it should obtain: an approval of senior management to continue a business relationship; and information about the source of wealth and funds of a client or a beneficial owner, and take reasonable steps to verify the source of such wealth or funds.

If the Company determines that a client or a beneficial owner with whom it has carried out a single transaction, is a prominent political figure, then as soon as it is possible after the transaction, the Company will take reasonable steps to obtain information about the source of wealth or funds of a client or of a beneficial owner and check the source of such wealth or funds.
In addition, the Company will carry out a more extensive effective control of business relationships involving a prominent political figure, family members or close associates of such figure.
In addition, the risks associated with PEPs, also include risks of corruption. In connection with this, the Company will apply to the Corruption Perceptions Index of Transparency International on www.transparency.org and take appropriate actions to manage the increased risks of business conclusion with PEPs.

7.4. Correspondence business relationship

Due to the fact that very often it is impossible or impractical to obtain original documentary proof of identity, business with clients will be carried out by means of correspondence. In such cases, the Company will apply the following CDD procedures to ensure that:
a) witnessed documents have been provided;
b) additional documents have been requested and received to supplement those required from an applicant for business face to face;
c) an independent contact has been initiated and established with a client.

7.5. Non-cooperative jurisdictions

The Company will have a special attitude to the necessity of a stiffened CDD and additional procedures for monitoring a transaction and business relationships, which involve countries with a non-cooperative jurisdiction or countries, which are the subject of FATF public statements on deficiencies in their AML/CFT systems. (They are defined in Annex 2).
The Company will check FATF website on a regular basis to get updates on the aforementioned countries.

7.6. New or Developing Technologies / Products Favourable to Anonymity

Prior to establishing a business relationship or carrying out an occasional transaction, in which new or developing technologies, or new or developing products are involved, that might be favourable to anonymity, the Company, in addition to the requirements set out in Part III, must take any further measures that may be needed to in order to minimize and control risks of new and developing technologies, or new or developing products that might be favourable to anonymity, in order to prevent their use in crimes of money laundering or terrorist financing; and to ensure compliance with any other requirements prescribed by regulatory provisions and are related to a special technology or product.

PART V – PERSONS RESPONSIBLE FOR COMPLIANCE WITH AML/CFT

1. Assignment of responsibility for ensuring compliance with AML / CFT

1.1. The Company must appoint a person responsible for ensuring compliance with AML/CFT, which will be sent all internal reports about suspicious transactions, drawn up in a prescribed form, which can be found in Appendix 3 to this document. In appointing a person responsible for ensuring compliance with AML/CFT, the Company will become convinced that a company official possesses appropriate qualifications, experience, competence, authority and independence to be able to fulfill the obligation for reporting effectively and autonomously.
1.2. After the appointment of the Company ensures that the responsibility for ensuring compliance with AML/CFT:
a) it has an appropriate autonomy and independence;
b) it has access to all relevant materials in order to to make an assessment of whether a transaction/activity is suspicious or not; and c) an appropriate data reporting for the Board of Directors is performed.

2. The role of responsible persons for ensuring compliance with AML/CFT

2.1. The Company guarantees that a person responsible for ensuring compliance with AML/CFT has timely access to identification data of clients and other CDD information, reports on operations and other relevant information to properly assess internal reports of suspicious transactions.
When reporting to a Senior Manager of the Company, a person responsible for ensuring compliance with AML/CFT will be independent in his/her decision as to whether an external report on suspicious transactions to be sent to a Commissioner, and free to make his/her own decision, without undue influence, pressure or fear of consequences if his/her decision may not be accepted by higher-ranking colleagues.
2.2. Once an internal report on a suspicious transaction has been approved by a responsible person for ensuring compliance with AML/CFT, he or she will act in accordance with the obligation to send the report to a Commissioner.
2.3. Responsibilities of a responsible person for ensuring compliance with AML/CFT should at least consist of the following:
a) implementation and control over daily functioning of an AML/CFT program;
b) informing Board of Directors of any significant violations of the program and laws, codes and established practice of AML/CFT;
c) preparation of reports each year - or more frequent intervals - if necessary, for Board of Directors, which determines, among other things:

- compliance with/deficiencies of internal control and other applicable procedures of AML/CFT;
- recommendations to correct deficiencies identified according to the abovementioned;
- the number of internal reports compiled by the staff; o the number of external reports submitted to the Commissioner

PART VI – EFFECTIVE CDD & ACCOUNT MONITORING SUSPICIOUS TRANSACTION REPORTS

1. Effective control

1.1. Once identification procedures have been completed, and business relationship has been established with a client, the Company will control the relationship on an ongoing basis in order to:
a) ensure that business relationships and transactions relating to these business relationships are compatible with the Company's knowledge of a client and a client's profile in relation to business and risks;
b) identify any grounds for reporting about a suspicious transaction.
1.2. When conducting the existing CDD and taking a due account monitoring, the Company will:
a) consider the type of carried out CDD when relationship with a client has been installed, and a risk level;
b) on a regular basis, review the activities of a client's account and operational behaviour, as well as information about a client received in accordance with these instructions.
1.3. Controlling actions and transactions of a client, the Company will conduct periodic reviews of existing reports and ensure the relevance of information available with respect to business relationship. Such reviews will also be used as a basis for identifying schemes of unusual activities or transactions of a client. The Company also will pay attention to information or instructions received from a client before or during their processing.

2. Suspicious transactions

2.2. Indicators of a potentially suspicious activity Suspicious activities include, but are not limited to the following:
a) any activity that casts doubt about the true character of an applicant for business or their managers;

b) any relationship or agreement, which seems to have no clear business justification or explanation;
c) any unusual or inexplicable transaction in the context of a normal example for a special relationship;
d) reluctance on the part of clients to respond to the investigation conducted by the Company;
e) unusually related transactions;
f) transfers of funds to or from accounts in countries, which are known to be associated with drug trafficking or other serious crimes;
g) any activity that does not seem to correspond to CDD information and a client profile, such as the apparent position and a client's funds;
h) clients who provide or carry out the collection of large amounts of cash money;
i) a request the use accounts of an intermediate client as bank accounts;
j) settlement of transactions using cash money or bearer instruments.
Employees of the Company will fulfill their legal obligations for the purposes of AML, revealing their suspicions to a person responsible for ensuring compliance with AML/CFT, providing Internal Disclosure Statement / Report on Suspicious Transactions (Annex 3).
If a person responsible for ensuring compliance with AML/CFT to approves the report, he/she will draw up his/her own report on this and on related circumstances as soon as possible, but not later than 3 business days after the formation of a suspicion, sending it to a Commissioner, in accordance with the section "Report on Suspicious Transactions".

2.3. Report on Suspicious Transactions

Report on Suspicious Transactions shall:
a) contain the reasons on which the Company supports their suspicions;
b) be signed by a person responsible for ensuring compliance with AML/CFT (if the report is not sent by e-mail or any other similar means of communication);
c) to the Commissioner by means established between the Company and an appointed Commissioner.
If the urgency of the situation requires it, the Report on Suspicious Transactions may be made orally to any police officer authorized for this purpose by the Commissioner, but in any such case, the Company shall, as soon as possible, but no later than 3 working days, send the Report on Suspicious Transactions to the Commissioner which meets the requirements of subsection (1).
Once the internal Report on Suspicious Transactions has been directed to a person responsible for ensuring compliance with AML/CFT or the Report on Suspicious Transactions has been provided to the Commissioner, the Company is ensured that due attention is paid during the following inquiries in order to prevent a client to learn about the disclosure, in case of the Commissioner's request for obtainment of additional information relating to suspicious transactions.

PART VII – RECORD KEEPING

1. Obligation to keep records of transactions

1.1. Regarding each transaction, which is held with the Company, the Company shall keep records of transactions so that a transaction can be restored at any time. Reports on transactions include, but are not limited to the following information:
a) nature of a transaction;
b) a transaction amount and currency in which it has been expressed;
c) a transaction date;
d) transaction parties;
e) if possible, means through which a transaction has been carried out, and any other instruments directly involved in the transaction;
f) a source and destination of funds, including full information on a remitter (instructions, forms of authority, agreements/contracts, where applicable);
g) name of a company official or an employee of the Company, who has performed a transaction or has had business relationship face to face in relation to transactions with any of the parties of a transaction and has formed a suspicion about a transaction, which would give the foundation to draw up a Report on Suspicious Transactions.
1.2. All records of transactions are kept, including those related to one-time transactions, for a period of at least 5 years after completion of a transaction, or any longer period that may be determined by an authorized body.

2. Obligation to keep a record of identification and verification

2.1. The Company will retain copies of all documentation used to verify the identity of all applicants for business. Records of identification will be stored for a duration of each relationship and within a period of time provided for in this section. These reports will include the following:
a) copies of identification data obtained in order to verify the identity of all clients, beneficial owners and main executives; and
b) copies of any client's files, their records on accounts, business correspondence and information relating to business relations; or
c) information related to the source where copies of identification data and other files can be obtained.
2.2. All records of identification and identity verification will be kept for a period of at least 5 years after completion of business relationship, or for any longer period which may be determined by a Commissioner.

3. Obligation to keep records of a different type

3.1. In addition to the reports referred to in sections 1 and 2 above, the Company will maintain and keep:
a) records related to establishment of business relations;
b) records related to risk assessments, AML/CFT programs and audits;
c) internal reports of a suspicion received a person responsible for ensuring compliance with AML/CFT;
d) reports on measures taken in accordance with internal and external reports of a suspicion;
e) all reports prepared by a person responsible for ensuring compliance with AML/CFT for a Commissioner;
f) records related to AML/CFT training of personnel;
g) reports of a person is responsible for ensuring compliance with AML/CFT for Board of Directors and senior management, and reports on examination of such reports and any measures taken in response to the latter;
h) any other reports (e.g., files on accounts, business correspondence, and written data) related to or received in the course of business relations, which are necessary to establish the nature and purpose of business relationships and activities associated with the latter.
3.2. The Company will keep records of the above-mentioned documents for at least 5 years after completion of business relationships or after the occurrence of any of the events specified in this section.

4. How to keep records

Records established by Law will be carried out in writing in English and will be ready to be converted into written form in the English language.

5. When keeping records is not necessary

Keeping records is not necessary if the Company has been eliminated and has completely stopped its activity except for cases where Supreme Court may issue an order requiring that any or all of the reports are stored for any period that it considers to be appropriate.

6. Destruction of records

After expiration of a period during which the Company is required to maintain reports, each report and each copy of a report will be destroyed, if there is no a legitimate reason for the preservation of this report, which may be necessary:
(a), in order to meet the requirements of any other directive; or
(b), to allow a subject of initial financial monitoring to conduct its own business; or
(c) for the purpose of detection, investigation or prosecution in respect of any crime.

PART VIII – TRAINING AND CULTURE

1.1. Awareness and training

The Company will see to it that its employees are aware of:
● the Company policy, procedures and management for AML/CFT;
● their legal obligations, the value of failure to provide information in accordance with the established procedure and a potential criminal liability in accordance with laws, regulations and recommendations of AML/CFT;
● developments of methods, techniques and tendencies of money laundering and terrorist financing.
The Company will make sure that all of its employees will be informed about a person responsible for ensuring compliance with AML/CFT, as well as about the responsibilities of the latter.
Employees provided with AML/CFT program, must fully understand the program and its importance. This will allow an employee to understand the procedure of registration of a Report on Suspicious Transactions.
A person responsible for ensuring compliance with AML/CFT will provide appropriate training so that employees can perform their duties in relation to AML/CFT, respectively, in particular to evaluation of information in order to to determine whether an activity or a business relationship are suspicious. This training will include, among other things, identification, processing of suspicious transactions and adoption of additional measures and will be aimed at maintaining of a high level of awareness and vigilance between educational seminars.

1.2. Selection and recruitment of employees

In order to prevent and detect money laundering and terrorist financing, the Company will apply the appropriate procedures to ensure competence and integrity of its staff. In particular, when hiring employees, appropriate measures of selection will be applied that will include without limitation the following:
● obtainment of recommendation letters and their confirmation when hiring new employees;
● confirmation of employment history and qualification;
● request for details of any disciplinary actions taken against a person, or absence of such measures taken by previous employers or any professional organization;
● request for details of any criminal record (or lack of a criminal record) and its confirmation, if possible.
New employees will get an introductory training on money laundering and terrorist financing, as well as a clear indication of the importance of issues related to money laundering and terrorist financing.
Employees will also be aware of legal requirements for reporting of suspicious transactions/activities, and procedures for reporting to a person responsible for ensuring compliance with AML/CFT, before they will be actively involved in daily operations.

1.3. Relevant personnel

Employees whose duties relate to processing of transactions or business relationships, will be separated from the full staff of the Company.
The latter will be respectively designated as “relevant personnel”. When determining whether an employee belongs to the “relevant personnel”, the Company will take into account the following:
a) if an employee performs any client functions or is responsible for conducting business relationship or transaction processing; or
b) whether an employee supports directly a colleague, who performs any of the functions referred to in paragraph (a) above.
In view of the fact that the Board of Directors and senior management are responsible for effectiveness and appropriateness of the Company’s policy, procedures and controlling means to counter money laundering and terrorist financing, all directors, managers and persons responsible for ensuring compliance with AML/CFT will also be considered as the “relevant personnel”, who have to carry out a continuous training in order to to maintain competence and to pay appropriate attention to assessment of effectiveness of the mentioned policies, procedures and control means.

1.4. Continuing training

The “relevant personnel” will act in accordance with obligation to obtain a continuing education that is compatible with their role and responsibilities. This training will include:
a) legal obligations, as well as all aspects of laws, instructions and AML/CFT recommendations;
b) weaknesses of products and services offered by the Company, concerning the issue of money laundering and financing of terrorism;
c) CDD requirements and requirements for internal and external reporting on a suspicion;
d) detection and processing of suspicious transactions/activities; e) existing criminal sanctions in case of refusal to provide information;
f) new developments, including information on current techniques, methods, trends and typologies of money laundering and financing of terrorism;
g) information about changing behaviour and practices among people involved in money laundering and financing of terrorism.
Training frequency will be determined on the basis of risks, and the employees responsible for handling business relationships or transactions, undergo training more frequently. However, a training workshop will be held at least once a year.

1.5. Training of a person responsible for ensuring compliance with AML/CFT

Since the responsibility for ensuring compliance with AML/CFT contains a significant responsibility for the acquisition, evaluation and external reporting on suspicious transactions, he or she should receive additional training, comprehensive and specific, taking into account the following:
a) detection and processing suspicious transactions;
b) cooperation with law enforcement agencies; and
c) reporting risk management.
A person responsible for ensuring compliance with AML/CFT will examine on a regular basis FATF Reports on money laundering typologies, which explore tendencies of money laundering activities.
He or she will also be aware of those countries which according to FATF have deficiencies in their AML/CFT systems.

1.6. Culture

The prevailing culture of organization can create certain barriers, which can lead to inappropriate handling of relationships involving criminally derived property. Inadequate compliance culture can be manifested in many ways, for example:
● attitudes among minor employees who believe that their suspicions and concerns carry no consequences are especially dangerous since minor employees in fact often are related to daily activities with operations;
● inability to appropriately and clearly record stored information on CDD;
● administration pressure for carrying out a transaction;

● eagerness to attract new business relationships;
● reluctance to expose important customers the same degree of vigilance.
The Company will take appropriate measures to prevent these and other barriers, and will encourage and support all staff members to be alert and attentive towards the occurrence of any illegal actions.

Annex 1

Client Declaration Form

Client's name:

Client's address:

Date: _____
Place: ____, _____

1) I _____ understand that I am making this declaration for my own protection as well as for the protection of Comax Invest Limited;

I declare that the data provided to Comax Invest Limited is complete and true and I have full legal capacity and sufficient knowledge to enter into agreements and use Comax Invest Limited services;

I declare that original or certified copy of CDD will be available at request without delay and undertake to inform Comax Invest Limited of any changes in the data provided within 30 days from the date the changes occurred;

I declare that I am an ultimate beneficial owner (not a nominee or trustee for any other person) of the funds to be deposited by the undersigned to Comax Invest Limited. The funds that will be transferred to Comax Invest Limited are obtained legally by the undersigned from the following source (s):

_____

_____

_____

I declare that services provided by Comax Invest Limited will not be used to achieve any criminal goals, including money laundering and terrorism financing.

2) Status

[ ] Resident of Marshall Islands
[ ] U.S. resident
[ ] Politically exposed person (PEP)
[ ] Person under personal sanctions
[ ] Other (specify) _____

3) Legally accepted clients identification documents

Expiry Date

[ ] A valid driver's license and its expiry date: _____

[ ] A valid identity card and its expiry date: _____

[ ] A valid passport and its expiry date: _____

[ ] Another document to be designated by the Minister and its expiry date: _____

----------/----------

(Client's signature)

Annex 2

COUNTRIES HAVING DEFICIENCIES IN AML/CFT

1. Albania
2. The Bahamas
3. Barbados
4. Botswana
5. Cambodia
6. Ghana
7. Iceland
8. Jamaica
9. Mauritius
10. Mongolia
11. Myanmar
12. Nicaragua
13. Pakistan
14. Panama
15. Syria
16. Uganda
17. Yemen
18. Zimbabwe

Annex 3

INTERNAL REPORT OF INFORMATION DISCLOSURE TO A PERSON RESPONSIBLE FOR COMPLIANCE WITH AML/CFT

1. Reporting employee
Name: ……
Telephone number: ……..

2. Client
Client's name: ……..
Address:…….
Contact name: ……..……..
Contact telephone number: ……..
Date of establishment of a business relationship ……

3. Information/suspicion
Suspected information: ……
Transaction: ……..
Ground for suspicion: ……

Please attach copies of any relevant documents to this report.

Signature of reporting employee: …… Date: ……..

Informing the client/customer or any other person about your suspicion and report is a crime.

This report will be considered in the strictest confidentiality.

For a PERSON RESPONSIBLE FOR COMPLIANCE WITH AML/CFT:

Receipt date: …… Receipt time: …… Ref: ……..
Authorized body is notified:
Yes/No
Date: …… Ref: ……