LESCOVEX

Trading platform for the creation
and exchange of digital assets

Manual for the Prevention of Money Laundering and Countering the Financing of Terrorism

Incorporated in Switzerland

Table of contents

I. Introduction

In response to the international community's growing concern about the problem of money laundering and the financing of terrorism, many countries around the world are enacting or strengthening their laws on the subject.

Along with society and the authorities of different countries, **LESCOVEX EXCHANGE, S.A.** (hereinafter "**Lescovex**" or **"The Company"**) recognizes the importance of the fight against money laundering and terrorism financing, since it impacts fundamental aspects of social life.

Lescovex understands that the best way to fulfill this commitment is to establish effective internal policies and procedures that are conducive to: 1) Carry out the activities and services provided in accordance with strict ethical standards and current law regulations; 2) The implementation of codes of conduct and monitoring and reporting systems to prevent **The Company** from being used for money laundering and terrorism financing; 3) Ensuring that all the employees observe "Know Your Customer" policies and procedures; 4) Strict compliance with applicable anti-money laundering and terrorism financing laws, as well as the recommendations issued on this subject by the International Financial Action Task Force and international and Switzerland authorities.

As a result, **Lescovex** management and employees must be vigilant for any suspicious activity and report it immediately to the established internal bodies, in accordance with specified policies and procedures, so that they may in turn notify the relevant authorities.

Only through the commitment of all **Lescovex** executives and employees will it be possible to guarantee that the products being marketed and the services being provided cannot be used for money laundering or terrorism financing purposes.

Adherence to this policy is absolutely fundamental to ensuring that **Lescovex**, comply fully with anti-money laundering and terrorism financing legislation. **The Company** should therefore be actively involved in the policy's implementation and development.

This policy establishes minimum standards which **Lescovex** should observe and is defined according to the principles contained in the 49 Recommendations of the International Financial Action Task Force (FATF), Swiss Federal Act on Combating Money Laundering and Terrorism of 10 October 1997 (AMLA) and the obligations and principles of European Parliament and Council Directive 2005/60/RC dated 26th October 2005, regarding the prevention of the use of the financial system for money-laundering and the financing of terrorism.

Compliance with the contents of this Manual is required for all **LESCOVEX EXCHANGE, S.A.**'s executives and employees. Non-compliance with the criteria and guidelines contained in this Manual will lead to the corresponding responsibilities and sanctions.

The contents of the Manual will prevail over other internal regulations that could come in conflict with these, excepting those that establish more strict conduct and/or prevention measures

II. Enforceable law

A. International law

- **The Financial Actions task Force (FATF)**. It is the main international body established to combat money laundering and terrorist financing. It has issued the "Forty Recommendations" report and the "Nine Special Recommendations on Terrorist Financing" report. The international community considers these to be the universal standards;

- **The Basel Committee.** It develops standards, guidelines and best practices for a wide range of banking supervisory matters. It has issued three documents on to the prevention against money laundering: 1) "Prevention of Criminal Use of the Banking System for the Purpose of Money Laundering" (1988); 2) "Customer Due Diligence" (2001); and 3) "Know your Customer Risk Management" (2003);

- **Wolfsberg Group Principles:** Statement Against Corruption (2007); Risk Based Approach for Managing Money Laundering Risks (March 2006); Statement on Monitoring Screening Transactions (September 2003); Anti Money Laundering Principles for Correspondent Banking (November 2002); Statement on the Financing of Terrorism (January 2002); Anti Money Laundering Principles for Private Banking (Revised version May 2001);

- **Directive 2005/60/EC of the European Parliament and of the Council of 26th of October 2005** on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing;

- **Commission Directive 2006/70/EC of 1st of August 2006** laying down implementing measures for Directive 2005/60/EC of the European Parliament and of the Council as regards the definition of 'politically exposed person' and the technical criteria for simplified customer due diligence procedures and for exemption on grounds of a financial activity conducted on an occasional or very limited basis.

B. Swiss law

- **Federal Act on Combating Money Laundering and Terrorism of 10th October 1997** (AMLA);

- **Swiss Criminal Code of 21st December 1937** (SCC).

III. Definition of money laundering and financing of terrorism

A. Definition of Money Laundering and Laundering of Assets

Asset laundering is also referred to as money laundering, whitewashing, laundering of capital, legitimizing capital, laundering of assets, etc.

All of these terms refer to the same process that is defined by the art.305bis of the Swiss Criminal Code as: "An act that is aimed at frustrating the identification of the origin, the tracing or the forfeiture of assets".

The Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, describes Money Laundering as the following activities:

1. *"The conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such activity to evade the legal consequences of his action.*
2. *The concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from criminal activity or from an act of participation in such activity.*
3. *The acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such activity;*
4. *Participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions mentioned in the fore- going points."*

As for United Nations Money Laundering is: "The surreptitious introduction of illegally obtained funds into the legitimate channels of the formal economy".

International Monetary Fund consider that "Money laundering is the process through which assets obtained or generated as a result of criminal activities are transferred or disguised, with the purpose of concealing their ties to crime".

Generally speaking, the money laundering process, very closely linked to the financing of terrorism, consists of three stages:

Placement: Introduction of cash originating from criminal activities into financial or non-financial institutions.

Concealment: Separating the proceeds of criminal activity from their source through the use of layers of complex financial or non-financial transactions. These layers are designed to hamper the control of the funds, disguise their origin and provide anonymity.

Integration: Placing the laundered proceeds back into the economy in such a way that they re-enter the financial system as apparently legitimate funds.

Given the nature of the financial operations used for laundering money, it is possible that financial entities be used inadvertently as agents for investing funds coming from illicit or criminal activities, jeopardizing the stability, reliability and credibility of the institutions involved.

B. Definition of Financing of Terrorism

The United Nations has defined terrorist financing as the following:

"A person by any means, directly or indirectly, unlawfully and willfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out:

(a) An act which constitutes a offence within the scope of and as defined in the existing treaties; or

(b) Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act."

In this sense, the Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, describe Terrorism Financing as follows: "the provision or collection of funds, by any means, directly or indirectly, with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out any of the offences within the meaning of Articles 1 to 4 of Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism".

Finally, the art.260quinquies of the Swiss Criminal Code, in a similar vein as the foregoing, take into account the foregoing definitions and defines Terrorism Financing as: "Any person who collects or provides funds with a view to financing a violent crime that is intended to intimidate the public or to coerce a state or international organisation into carrying out or not carrying out an act is liable to a custodial sentence not exceeding five years or to a monetary penalty".

IV. Company identification

Company Name: LESCOVEX EXCHANGE, S.A.

Registered Office: Villa Décentrale, 59, 2610 Mont Soliel (Saint Imier)

Register Number: CHF-393.870.130

Business Purpose: The Company shall have as its main purpose the operating of an Exchange platform based in blockchain technology in which different cryptocurrencies may be exchanged, as it is set forth on the website: www.lescovex.com.

Contact:

Email: support@lescovex.com

Phone number: +41 78 726 14 31

V. Customer identification and know your customer policy

A. Definition of Customer

Regardless there is no official definition of customer in the regulatory bodies aforementioned, to the effect of this Manual we consider by "Customer" the following: *"any person, natural or legal entity, who has passes successfully all the Know Your Customer and Due Diligence procedures established by* **The Company** *and with whom* **Lescovex** *has a business relationship, offered under the scope of activities provided proper to the field of its expertise and in compliance with established legal and regulatory framework".*

B. Customer Acceptance Policy

Lescovex shall lay down a customer acceptance policy, which shall include a customer classification attending to different risk factors in which they may incur (activity carried out, country or residence, etc.). In that sense, **The Company** shall not admit as customer nor, therefore, establish a business relationship with the following persons, whether individual or legal entities:

1. Those persons about whom information is available indicating possible evolving in criminal activities or which are included in any public list concerning to criminal activities (such as US Office of Foreign Assets Control –OFCA-, etc.), mainly related to drug trafficking, terrorism and organized crime;
2. Persons with businesses that due to the nature of the business make it impossible to verify its legitimacy or the source of its funds or those which funds are inconsistent with their financial status;

3. Persons who refuse to provide the information or documentation required to obtain verification of the activities or the source of the funds or who provide documentation of doubtful legality or legitimacy or which have been manipulated;
4. Legal entities whose shareholder or control structure cannot be determined;
5. Casinos, gambling/betting establishments, exchange offices, money transmitter and other similar entities that are not officially authorized;
6. Financial institutions resident in countries or territories without being physically present (also referred to as "shell banks") and which do not belong to a regulated financial group.

For another side, the following persons, whether individual or legal entity, shall only be accepted as customers by **The Company** with prior authorization from Compliance Officer of **The Company**:

1. Customers involved in the production or distribution of weapons or other military equipment;
2. Duly authorized casino, gambling establishments or Bureaux de change, money transmitters or other similar entities;
3. Customers who are high-level public officials and their family members or close associates as defined in art.2a of the AMLA (Politically Exposed persons "PEP's").

C. Risk Factors

For Money-laundering and Terrorism financing, **The Company** shall take into account different risks factors at the time of evaluating and verifying the information and documentation facilitated by customers and depending on those Lescovex shall classify its customers in Low, Medium or High Risk Customers. Those risk factors are, among others, the following:

1. **Geographic location:** There are certain geographic locations considered as higher risk for money laundering and terrorist financing, such as those that are not members of the Financial Action Task Force (FATF), or regional FATF like bodies groups of similar nature; and those countries being subjected to sanctions by the aforementioned groups for not being compliant, or not being sufficiently compliant with FATF recommendations.

   Customers considered as high risk due to their geographic location are those who have substantial connections in a high risk country/city, that is: a) Those who hold property, residence, offices or headquarters in a high-risk country; b) Companies which the majority shareholders or beneficiary owners are located in such countries; c) Any other substantial connections/links

   that might be identified. Although Nationality is

   an important element it is not determining to classify someone as a high risk customer.
2. **Activity:** There are certain business and/or industrial activities that due to their nature are more likely to be used for money laundering and terrorist financing. Some activities considered high risk are as follows: Casinos, Gaming Centers, Racetracks; Financial Investment Corporation (S.A.F.I.); Arms, weapon manufacturers, distributors and dealers; Precious metals distributors and dealers; Professionals who act as intermediaries (Lawyers or accountants that manage their customer's funds in their accounts); etc.

   It shall be considered as a High Risk Customers those who possess significant connections to activities considered high risk. The Compliance Officer will have to determine whether the connection is significant or not. There is always a significant connection if **The Company** is involved in or if a large portion of **The Company**'s turnover comes from high risk activities.

1. **Politically Exposed Person (PEPs)**: Public corruption is considered as prominent cause for money laundering. This is why having ties with people who hold or have held prominent public functions or others who are closely connected with them, family members or close associates, might pose a legal or reputational risk to our Company. Politically Exposed Persons (PEPs) as is defined in the art.2a of AMLA are:

"a) Individuals who are or have been entrusted with prominent public functions by a foreign country, such as heads of state or of government, senior politicians at national level, senior government, judicial, military or political party officials at national level, and senior executives of state-owned corporations of national significance (foreign politically exposed persons);

b) Individuals who are or have been entrusted with prominent public functions at national level in Switzerland in politics, government, the armed forces or the judiciary, or who are or have been senior executives of state-owned corporations of national significance (domestic politically exposed persons);

c) Individuals who are or have been entrusted with a prominent function by an intergovernmental organisation or international sports federations, such as secretaries general, directors, deputy directors and members of the board or individuals who have been entrusted with equivalent functions (politically exposed persons in international organisations);"

Having business relationships with PEPs family members, close associates, or companies controlled whether directly or indirectly by PEPs represent risks to the reputation of **The Company** similar to those damages caused to the reputation of PEPs themselves.

3. **Materially:** The materiality of the relationship with a customer is also a risk. In order to evaluate it, **The Company** will attend to the volume or amount of transactions channelled through the **Lescovex** platform, the source of the funds and the funds in their financial status. It is also set a limit funding to control those transactions, over which customers to carry them out must obtain an authorisation.

4. **Legal Entities:** Relationship with legal entities may pose a risk for **The Company**, as persons who directly or indirectly control those entities may use them to hide their identities and carry out illegal activities related to money laundering or terrorism financing.

In such cases, additional due diligence procedures are required in order to know the **beneficiary owners** of the legal entity, the type of operations of **The Company**, the purpose of using **Lescovex** platform, the source of the funds channelled through **Lescovex**, etc.

It is considered as a beneficial owner those natural persons who ultimately control the legal entity in that they directly or indirectly, alone or concert with third parties, hold at least 25 % of the capital or voting rights in the legal entity or otherwise control it. If the beneficial owners cannot be identified, the most senior member of the legal entity's executive body must be identified.

In addition, for record keeping purposes and to know our customers, we shall request information that will allow us not only to identify and validate the identities of the Beneficiary owners of the entity and the funds of the latter, but also to monitor their financial, business activity and the source of the funds channeled through **Lescovex**.

D. Customer's identity verification

The Company considers that the most effective means of preventing the use of our services from money laundering or terrorism financing is to identify and apply "know your customers" (hereinafter "KYC") procedures, including enhanced due diligence for those customers presenting higher risk, such as Politically Exposed Persons (PEPs), irrespective of whether they are established customers or otherwise.

KYC and all due diligence procedures followed are not a mere formal requirement that can be met simply by filling out a form. Nor it is a passive transaction where **The Company** simply requests information and documentation and the Customer provides it. But instead, it is a dynamic, ongoing process by which **The Company** requests information, screens it to make sure it is complete and requests supporting documentation when it is pertinent to do so. The information is then validated and finally all the documentation and data collected are evaluated to make sure they are consistent.

To verify the identity of the customer, **The Company** will apply different procedures of KYC:

a) Paper-based verification:

This is the common approach among digital assets exchanges across the globe. Users must provide personal details and upload several related documents such as passports, ID cards and proof of residence documents, which include bank statements or utility bills. Then, **The Company** verifies that all the personal details and submitted documentation match with the information stored in the identification documents' Machine-Readable Zone (MRZ). If so, **Lescovex** screen on users are not under any of the factor risks. If any, additional documentation and information may be required to admit them as customers.

b) Blockchain Certification Authority (BCA):

Another way to certificate the identity of customers is by using **Lescovex** BCA desktop application. The latter enables users to sign the KYC form with their qualified electronic signature issued by authorized entity, within which, it is included all the personal details of the customers.

BCA integrates a method to add trusted certification entities (e.g. from governments and banks), and their root certificates into a smart contract run on Ethereum's blockchain. **Lescovex** easily and securely adds these root certificates into the smart contract. Corporations and individuals then submit their identity certificates that are verified by the BCA smart contract once the root certificates and those submitted match.

Since encrypted root certificates are of public domain, it is not necessary to trust the entity responsible for managing the contract. Anyone can query vetted fingerprints by the smart contract and, thereby, confirm whether they are the same as in the official website or database available of the certification entity which issues those certificates.

After recording the fingerprint and the public key of the certification entity, it is possible to confirm, unequivocally, that the certificates submitted by users relate to the root certificates, and thus attest whether entities have performed the pertinent controls necessary to validate the identity of any corporation or individual.

c) Video Identification:

Apart form the foregoing, in both cases, **Lescovex** will carry out an audio-visual real-time (live transmission) communication with customers to verify their identity. The transmission will be recorded and filed in **The Company**'s database. Customers will have to answer to targeted questions related to the personal details they have provided in the KYC form

set forth in the following section. Additionally, they will have to show the documents uploaded during the onboarding process, so that **The Company** can take a photograph of them during the transmission. For that purpose, it will be used a facial recognition application called "Open Computer Vision", which allows to take snap shots. The communication will be conducted through either Skype or Google Hangout application.

Before starting with the aforesaid procedure, **The Company** will have to obtain an explicit consent from the customer to carry out this communication, record it and take photos meanwhile. If the consent is not obtained, customer may ask for passing through a conventional identification procedure, by which they will have to send an authenticated copy of an identification document by postal delivery or other equivalent method.

E. Registration Process

Any person, natural o legal entity, who wants to become a customer and, therefore, use the services provided by **The Company**, must follow all the steps laid down on **Lescovex**'s website: **www.lescovex.com** and provide all the information and documentation required. Those steps are:

1. Sing up on the website **www.lescovex.com**: Customers will be asked for introducing a valid e-mail address and a password. Then a message shall be sent to the email address provided so as to validate it by clicking on the link sent together with the aforesaid message.
2. Once the e-mail account is validated, customers shall have to create a **Lescovex** account whether a "Personal Account" or a "Corporate Account":

A) **PERSONAL ACOUNT**: Customers must verify their identity whether by following the paper-based procedure or by signing the KYC form with the BCA desktop application. In the former case, customers must to fulfil the "know your customer form" (hereinafter "KYC form") displayed on the website, where personal information shall be required, such as name, last name, ID or Passport number, date of birth, address, City, Nationality, occupation, monthly income, if they are citizen, resident or tax payer of the USA, etc.

Those customers who have verify their identity by using the BCA procedure must also fulfil a KYC form to provide other information which is not include in the electronic certificate, such as occupation, monthly income, annual income, etc.

In addition, customers must upload a copy of their ID or Passport in colour and with a photo of themselves. This documentation must have an MRZ (Machine-readable Zone) and optical security features. The copy must be a readable copy so as the date of issue, date of expiration and date of birth of customer can be read easily. Expired or deteriorate copies shall not be accepted.

They must also upload a bank statement, tax bill, utility bill or so as a proof of residence. The address shown in this document must be the same as the one indicated in the form fulfilled or in the BCA signature.

Finally, apart from the foregoing, identification will be channelled via audio-visual real time (life transmission) communication between the customer and **The Company**. This audio-visual interview will be made through Skype or Google Hangout application. An explicit consent must be obtained from the customer so as to conduct this audio-visual identification, to record it and to take photos meanwhile, before starting the video interview.

Customers will have to answer targeted questions related to the information provided in the KYC form, as well as to show the documents uploaded, so that **The Company** can check whether the docu-

ments match with those provide on the onboarding process by reading and decrypting the information stored in the document's Machine-readable Zone. To that effect, **Lescovex** will use the "open computer vision" to take snapshots of the interview when customer is showing their documents, so as to get a facial recognition of the customers and check the authenticity of the documents shown.

Customers may ask for any other conventional channel to carry out the verification process, such as sending an original notarized copy of their documents by postal delivery.

In some cases, and due to the type of customers, especially those who might fall under one of the risk factors set forth before, **The Company** may enhance the due diligence by asking for more information or documentation in order to decide whether to admit or not them as a customers.

B) **CORPORATE ACCOUNT**: Companies must also verify their identity, whether by using the paper-based procedure or by using the BCA. If they choose the first option, the person who is acting on behalf of **The Company** shall have to fill out the KYC form for Corporate Accounts displayed on the website, where, among other, will be required the following information:

1) Company's name;

2) Company's registration number or Tax ID, if different;

3) Company's website (URL);

4) Registered address;

5) City; 6) Postal Code;

7) Country;

8) Main purpose of the account:

(i) Accepting or converting payments from customers for services rendered of good sold;

(ii) Depositing or withdrawing funds to business account;

(iii) Managing funds or other individuals; (iv) Any other business activities, must be specify.

As in the foregoing case, when users verify their identity by BCA procedure, they must also to fulfil the KYC form in order to provide that information that is not obtained by the aforementioned procedure.

Apart from that, **Lescovex**'s support staff shall send a message to the contact email address provided asking for more information and documentation to verify and validate **The Company** customer. This documentation could be sent, whether by postal delivery, provided it's the original one, or by email, provided is signed with a qualified electronic certificate pursuant to Federal law on certification services in the area of electronic signature of 19th December 2003:

- Powers of attorney of the person who is acting on behalf of **The Company** customer during the process of creation of **The Company** account. If it is **The Company**'s director, a notarized document of the appointment must be provided;
- Attestation of the entry in the appropriate register (Commerce Register normally);
- Memorandum of Association and Corporate bylaws or articles of association;
- Copy of the taxpayer register;
- Statement of the director or board of directors' agreement by which they expressly declare the willing of acquiring LCX token from **Lescovex**. A copy of the ID (front and back), or passport must be attached to this statement.

- Affidavit stating the following issues:
  - Business activity and services provided.
  - Typical customer profile.
  - Type of systems payments accepted and the price of the services;
  - Specify the purposes of opening an account in **Lescovex** and using its services;
  - The type of trading is going to be carried out in **Lescovex** platform;
  - Identification of the shareholders, specially the beneficial owners, considering them as those natural persons who ultimately control the legal entity in that they directly or indirectly, alone or in concert with third parties, hold at least 25 % of the capital or voting rights in the legal entity or otherwise control it. If the beneficial owners cannot be identified, the most senior member of the legal entity's executive body must be identified (full name; last name; address; postal code; ID –front and back- or passport number; Readable copy of the ID or Passport).
  - Identification of **The Company**'s Directors (full name; last name; address; postal code; ID or passport number; Readable copy of the ID or Passport);
  - Source of funds of **The Company**;
  - Name, address and SWIFT code of the legal entity's bank;
  - If your business is AML regulated. If so, state your policy and how **The Company** perform KYC for your customers and any other due diligence measure. Additionally, provide us with your AML and CFT Policy;
  - Estimated monthly volumes, amount in CHF (last two balance sheets must be attached);
  - Financial situation (balance sheet or any other related documents may be required);
  - State if **The Company** have another account opened in other cryptocurrency exchange.
  - How users can reach normally the services provided;

Depending on the characteristics of **The Company** and any other circumstances, **Lescovex** may enhance the due diligence and ask for any other information and documentation different from which have been set out before.

Apart from the foregoing, audio-visual identification through the process described in the previous section (Personal Account) will be carried out to check the identity of the person who is acting on behalf of **The Company** customer.

F. Funding Limits

Individuals who has verified their account following the aforesaid procedure will be allowed to carry out deposit and/or withdraws under the following limits, over which they will have to contact with **Lescovex**'s support staff (support@lescovex.com):

	Daily Limits	Monthly Limits
Deposit Fiat	*20.000,00 CHF*	*150.000,00 CHF*
Deposit Crypto	*No Limit*	*No Limit*
Withdraw Fiat	*20.000,00 CHF*	*150.000,00 CHF*
Withdraw Crypto	*50.000,00 CHF*	*150.000,00 CHF*

As for the companies verified, they will be allowed to carry out deposits or withdraws with the following limits, over which they will have to contact with **Lescovex**'s support staff:

	Daily Limits	Monthly Limits
Deposit Fiat	*150.000,00 CHF*	*600.000,00 CHF*
Deposit Crypto	*No Limit*	*No Limit*
Withdraw Fiat	*150.000,00 CHF*	*600.000,00 CHF*
Withdraw Crypto	*150.000,00 CHF*	*600.000,00 CHF*

In any case, whether **Lescovex** identify any suspicious transaction will ask for more information or documentation to the customer, and if necessary, a report will be filed to the Reporting Office.

In both cases, whether personal and companies accounts, the deposits or withdraws of FIAT will solely be allowed to their own bank accounts, never to third parties accounts.

G. Screen on the Sanctions Lists

The documentation and information provided by the customers shall be verified and evaluated by **The Company**, namely by the compliance officer. Customers who were under one or several of risk factors and those who compliance officer considers to do so, shall have to provide more documentation and information so the Compliance could decide whether to accept or not them as a customers.

Before deciding on whether accept or not a customer and in order to comply with the acceptance customer policy stated in this section, Compliance officer shall check all persons, natural or legal entities, against the watch lists. If some of the customer is found in one of the watch lists all ties of that potential customer with **The Company** will be terminated and a report to the Reporting Office in Switzerland will be issued. In case any potential customer is included in the PEPs list, the Compliance Officer approval will be necessary.

H. Updating information and documentation

The information and documentation provided must be complete, accurate and current, and must be kept up-to-date at all time so that it complies with the requirements of authenticity and certainty, as long as customer continues to be a user of the services provided by **Lescovex**, in all cases being its responsibility the lack of updating and the consequences that may arise from it.

Customer's information and/or documentation must be updated annually or under one of the following circumstances:

a) Lescovex modifies its customer identification regulations;

b) If customer information is insufficient or out of date;

c) At the request of the compliance officer within the framework of an ongoing investigation;

d) At the request of the auditors;

f) If there are any significant changes in the customer's behavior patterns.

No transaction will be carried out with the customer if their identification information is pending or out of date.

I. Follow-up of the Relationship with the customer

The type of transaction the customer conducts or requests as well as the amounts involved in such transactions should always be controlled to make sure they are consistent with the customer's business activity and the information provided, if the documentation available does not validate such transactions then appropriate records must be obtained in order to do so.

"Know Your Customer" should be enforced throughout the relationship with the customer, not just at the beginning of it. The factors to monitor are: types of transactions conducted, amounts involved and how these are carried out.

VI. Monitoring policy and suspicious transactions report

A. Definition of Suspicious Transaction

"Those transactions that, considering the practices and customs of the business activity in question, seem unusual, appear to serve no financial, business or other legal purpose and are extremely complex for no reasonable explanation as well as those financial transactions that involve funds of dubious source."

B. Detection and control of Suspicious transactions

Irrespective of the funding limits set froth in the previous section, **Lescovex** shall carefully examine all the operations and trasactions channeled through the platform in order to detect any unusual or suspicious transaction. To determine what is unusual or suspicious about a transaction, **Lescovex** shall mainly pay attention to those transactions which show a lack of correspondence with the volume of activity or operational previous records of the customer, provided that there is no economic, financial, business or legal purpose for carrying out them, based on the characteristics and business financial profile of the customer set during the registration process.

In addition, no transaction of Fiat to third parties will be allowed in **Lescovex** platform. It will solely allowed deposits or withdraws of FIAT that are made to the customer's bank account. If several persons own the bank account, these others will have to be identified and follow all the KYC procedure, so that **The Company** can know at any time who they are and screen them on any sanction list.

Thanks to the technology of Blockchain, **Lescovex** shall be able to examine, analyse and trace all the transactions performed, knowing at any time all the circumstances related to them. Thereby, the system shall verify several aspects of each transaction made, such as the amount, the digital address to and from which the transactions is performed, which allow **The Company** to identify any suspicious or irregular transaction, whether the address to which is sent the money is listed in a blacklist or the amount of the transaction does not correspond with the profile of the customer or otherwise.

The Company has established different mechanism inside its system to identify those transactions. Thus, all the addresses to which the money is sent are screened at any time to blacklists so **Lescovex** can verify if it is related to any illegal activities. **The Company** has also fixed a daily and monthly amount transactions, upon which an authorisation to carry out them must be obtained. Even the ones which are within the range of authorised are at all time controlled by the system, so that it is possible to check and verify any suspicious transaction made in **Lescovex** platform.

If any of those transactions is identified, a warning shall be generated by the system and the transaction shall be rejected or freeze. In addition, an "Internal Operation Report" will be issued by **The Company**'s employees, to which will be enclosed all the supporting documentation and evidence of their analysis and shall be sent to the Committee for Prevention of Money Laundering and Terrorism Financing (hereinafter "The Committee").

The Committee, namely the compliance officer, shall investigate the documentation related to the transaction reported. The analysis shall be carried out as deepness and quick as possible. After this investigation the compliance officer will submit the results to the Committee, which decide at last instance whether to communicate or not the transaction to the Reporting Office. If so, all the documentation and details related to the suspicious transaction shall be filed to the Reporting Office as is set out in the next section. In other case, the incidence shall be archived in **The Company** database.

The communicating employee of such situation will be notified in writing of the result of the study carried out in relation to the suspicions of money laundering or terrorism financing within a period not exceeding 7 business days from the receipt of the communication.

In compliance with the applicable regulations, it is totally forbidden the disclosure of both communications and the identity of the caller. Therefore, they will have the character of strictly confidential.

In turn, all members of **The Company** are warned of the absolute prohibition to reveal to the client or third parties that information has been transmitted to Reporting Office or that a suspicious operation is being examined. Failure to comply with the disclosure prohibition is classified as a very serious breach by current regulations, which may result in the application of the sanctions provided.

All communications of suspicious activities will be filed together with the subsequent study and monitoring of the specific case. Access to such files will be restricted to the components of the Control Body.

C. Investigation Procedure

Irrespective of th The investigation procedure shall be as follows:

a) Analysis Protocol:

1. Each suspicious operation studied by the Committee (Compliance Officer), will have an individualized file, which will be assigned a

denomination in accordance with the following model: case number according to order / year (i.e.: Exp 03/18) to facilitate its ordering. These records will refer to each operation investigated, client, reason for the alert, extension of data made if necessary, decision adopted for remission or file and reason, as well as any other data or background that will be relevant for evaluation. As well as the reference to other files that could be related by intervening the same individuals etc.

2. Priority will be given to those operations in which a greater number of risk indicators concur, or in which the risk is of greater intensity or relevance.

b) Analysis:

1. The documentation and information of the customer will be analyzed. The history of operations performed by the same will be reviewed previously in the register of operations of **The Company** in order to check the correspondence between amounts, destinations, documents provided, frequency, etc.

2. If the available information is insufficient to draw a conclusion about the suspicious nature of the operation, the Compliance Officer will go directly to the customer in order to request additional information or documentation that is required in each case. As well as, the Compliance can address to the person who reported the operation, with the same purpose.

3. In the case of detecting a lack of clear correspondence, the accreditation of the lawful origin of the funds must be requested.

c) Analysis outcome:

After its in-depth investigation, the Compliance Officer will submitt the researches results to the Committee, which will decide whether to communicate or not the incidence to the Reporting Office. In the affirmative case, the operation will be communicated by the Compliance Officer, enclosing to the Report the documentation that supports the research carried out. Otherwise, the incidence and all the detail related to it shall be archived in the database of **The Company**.

D. Suspicious Transactions Report (STR) to the Money Laundering Reporting Office Switzerland (Reporting Office)

If the Committee considers that there are enough evidences to consider the transaction or the operation is made to carry out an activity related to Money Laundering, Terrorism Financing or Fraud, the Compliance Officer shall file a report to the Reporting Office in timely form and manner. It shall be also reported those cases in which **The Company** have terminated any relationship with some customer due to reasonable suspicion on being involved in activity or even when some customer has not been accepted for being registered in some of the Official Lists of Sanctions.

Once the report has been filed, **Lescovex** shall act as is set out in the arts.9a and 10 of the AMLA, in order to execute or freeze the transaction carried out by the customer reported, and at all time shall act as is required by the Reporting Office.

E. Confidentiality

Lescovex shall not disclose the fact that information has been sent to or requested from the Reporting Office to any person involved or connected to the suspicious transaction or operation reported or to any third party, nor shall they make any reference whatsoever about the case.

The self-regulatory organisation to which **The Company** is affiliated and FINMA are not regarded as a third party.

Any actions taken connected to the prevention of money laundering or terrorism financing shall be treated with utmost reserve and confidentiality.

VII. Recording keeping

The following information and documentation must be kept by **Lescovex** for at least 10 years, so it can be available if it is ever requested by the Reporting Office, FINMA or any other authority:

1. Documentation obtained during the KYC and Due Diligence procedures for identification of customers, which shall be kept for at least 10 years after the termination of the business relationship with the customer;
2. Original documentation or certified copies of the transactions carried out by customers through the **Lescovex** platform and the information related to them for a minimum of ten years after the completion of the transaction or operation carried out.
3. Any Report of Suspicious transaction issued and the documentation and information attached to it shall be kept during the 10 years after of the date of the report.

Lescovex has its own database in which all this documentation and information shall be stored as so to guarantee the due conservation and location to be available for both internal control or authorities requirements. Once a person apply for being a **Lescovex** customer, its information and documentation shall be registered on the **Lescovex** database, where will be stored in an encrypted hard drive solely accessible by **Lescovex** by an internal VPN.

VIII. Staff training policy

Lescovex belives that one of the best tools to combat money laundering and terrorims financing is to create a culture of compliance and control among its staff. For this Purpose, this Manual and all the regulation issued by **The Company** related to Prevention of Money Laundering an Terrorims Financing will be part of the internal procedures of **The Company** and its knowledge and compliance shall be mandatory for all those who are part of it.

Lescovex's staff shall have access to the updated version of this Manual and other inetrnal regulation related to it and will be involved in the prevention task, for which they will be duly informed and instructed on the matter.

In the case of any legal or regulatroy modification or improvements in terms of Prevention of Money Laundering, Terrorism Financing or Fraud, the entire staff shall be informed of it so the new implementations can be applied and complied properly.

Courses aimed to inform and train **The Company**'s staff to learn about the policy and how to apply the procedures related to Prevent Money Laundering, and Terrorism Financing through **Lescovex**, shall be periodically provided to the staff by **The Company**.

IX. Organisational structure

To comply with the policies set forth in this manual and with the requirements of FINMA and other legal authorities regarding to the prevention against Money Laundering and Terrorism Financing, **Lescovex** shall set up the Committee for Prevention of Money Laundering and Terrorist Financing, which will be composed by three members:

1. Two members of the Board of Directors.
2. The Compliance Officer, the person, natural or legal entity, who may be a member of board of directors or other hired to carry out the tasks related to it.

The Board of Director will evaluate the performance of the Committee and the Compliance Officer annually.

A. Committee for Prevention of Money Laundering and Terrorism Financing

The Committee shall work as collegiate body responsible for planning, coordinating and safeguarding the compliance of the legal framework and the policies established in the Manual For Prevention of Money Laundering and Terrorism Financing (hereinafter "The Manual"). For this purpose, The Committee will have full access to any and all information and/or documentation it deems necessary in order to fulfill their duties.

The Committee shall meet at least each three months and deal with all the issues related to the implementation and compliance of the Prevention of Money Laundering and Terrorist Financing within **The Company**. When a particular issue related to it must be dealt with urgently, the Compliance Officer shall convene an extraordinary meeting of the Committee.

The Committee shall have, among others, the following duties and responsibilities:

- Draft the Manual for Prevention of Money Laundering and Terrorist Financing to be approved by the Boards of Directors;
- Reporting annually (through the Compliance Officer) to the Board of Directors regarding compliance to The Manual and all internal regulation related to Prevention of Money Laundering and Terrorist Financing of **The Company**, suggesting, in its case, any pertinent modification whether to improve them or to implement any legal modification, justifying the reasons and the manner to do so.
- Spread among the staff of **The Company** the information and documentation necessary in terms of Prevention;
- Design the training staff plan and its implementation;
- Acknowledge and promote compliance with the remedial measures to be taken based on the reports of Internal and/or External Audits regarding the prevention of money laundering and terrorist financing;
- Decide on enhancements to the monitoring and control measures suggested by the Compliance Officer regarding the prevention of money laundering;
- Analyze the "Internal Operations Reports" submitted by **The Company**'s staff and approve or dismiss relaying suspicious transactions to the Reporting Office;
- Cooperate with the Reporting Office so as to provide all the documentation and information required;
- Preserve all the documentation and information generated by all the transactions and operations reported following which is set in Section VII of this Manual.

B. Compliance Officer

This position shall be held by the person, natural or legal entity, appointed by the Board of directors. It may be possible to outsource the service by hiring any person who meets all the due capabilities to carry out the tasks related to it. To this effect, **The Company** will draft an agreement listing all the tasks and responsibilities assigned to the Compliance Officer.

The appointment of the Compliance Officer will be informed to the FINMA and the Reporting Office (detailing name, position and branch). If there are any changes or updates to this information, the FINMA and Reporting Office must also be notified, within 5 days after the Officer was appointed.

The Compliance Officer shall have, among others, the following responsibilities and duties:

- Convene the meetings of the Committee;
- File the reports to the Reporting Office regarding operations or transactions in which there is certainty or signs of money laundering or financing of terrorism;
- Receive the requirement from the Reporting Office to provide information and documentation and to execute the actions asked for;
- Implementation of the Manual.
- Monitoring transactions carried out by customers;
- Investigate reports of unusual transactions, as well as those detected in the centralized monitoring process.
- Keep the rest of the committee members informed of any circumstance that could alter the prevention policy contained here;
- Present before the Committee suggestions to improve or implement new procedures for The Manual;
- Keep informed and updated about all legal matters and regulations that affect **Lescovex** in their management of the prevention against money laundering.

X. Internal control system

Due to the nature of the services provided by **Lescovex**, the latter shall apply different methods to guarantee the security of the transactions and to avoid the platform from being used as system to perform any illegal activity.

Thereby, **The Company** will apply policies and procedures in the area of due diligence, document preservation, internal control and risk management so to prevent transactions related to money laundering and terrorism financing. Those policies and procedures, some of which has been set in this Manual, shall be spread among all the employees and executives of **The Company**.

The aforementioned policies shall include a description of those types of customers that could present a higher risk, taking into account the risk factors set forth above and those determined in accordance with the applicable international standards in each case. As it is been said, customer must to provide all the information and documentation required so **The Company** is able to verify their identities and establish a profile of each of its customers. If any of them is under any of the risk factors mentioned, **The Company** will enhance the due diligence by asking for more information or documentation to decide whether to accept or not a person as a **Lescovex** customer.

For another hand and in order to control the transactions made by customers, **Lescovex** shall pay attention to the transactions made by customers and its correspondance with the profile of each customer which has been established. If the system detect that any of the transactions made does not correspond with the profile of the customer, whether due to the amount, frecuency, and so on, the system will issue a warning and the transaction will be reported to the Committee as a suspicious transaction to initiate a investigation. To this effect, **The Company** has also established a daily and monthly amount of transactions, whether to deposit or withdraw cryptocurrencies or legal tender, upon which an authorisation must be granted by **The Company**, to keep in this manner all the transactions under control.

Lescovex shal also use the technology of blockchain to examine and analyse all the transactions made in the platform and check if any of the adresses to which the cryptocurrencies or legal tender is sent is listed in any of the public blacklists.

The Company will always verify that bank account to or from which the customers deposit or withdraw legal tender is owned by the customer and none else. If any other person is co-owner, **Lescovex** shall also ask for information and documentation related to that co-owner, in order to have the necessary information to know at all the time where the money goes.

In terms of security, transactions will not be made if customers are not verified and if they do not use the two-factor authenticator system, so it is guaranteed that the transaction is been made by them. Apart form that, an e-mail wil be sent to their e-mail account to verify if they have made that transaction.

The Committee shall be in charge to apply and develop this Manual and all the regulation and policies related to Prevention Of Money Laundeing and Terrorism Financing, keeping the aforementioned Manul updated at all time and available to the relevant authorities.

XI. External control

The most important commitment of **Lescovex** is compliance with all what is been set forth in this Manual and those other regulations and policies related to prevent the Money Laundering and Terrorism Financing. In this way, apart form the internal control measures established, **Lescovex** shall be audited by external audit entities, so it can be verified that the procedures to prevent money laundering and terrorism financing which has been established by **The Company** are effective and forceful.

This external audit will take place annually. **The Company** will entrust the external audit to those persons who meet the appropriate knowledge and are academically qualified to carry out the task.

The results of the verification will be recorded in a report, which will describe in detail the existing internal control measures, evaluate their operational efficiency and propose, if necessary, any rectifications or improvements.

The report will be submitted within a maximum period of three months from the date of issue to the Board of Directors, which will adopt the necessary measures to resolve the deficiencies identified.

The report aforementiones will be available to any authority during the following five year to the issuing.

Lescovex is an early-stage business project and therefore the information in this document might be subject to change without notice, and should not be construed as a commitment by **Lescovex**. **Lescovex** assumes no responsibility for any errors that may appear in this document. In no event shall **Lescovex** be liable for incidental or consequential damages arising from use of this document. This document and parts thereof must not be reproduced or copied without **Lescovex** written permission, and contents thereof must not be imparted to a third party nor be used for any unauthorised purpose.