Trading platform for the creation
and exchange of digital assets

Table of contents

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 the society and the authorities of various countries, **LESCOVEX, S.R.L.** (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) Carrying 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 that **The Company** is 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 with the recommendations issued on this subject by the International Financial Action Task Force and international and Romanian 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** complies fully with anti-money laundering and terrorism financing legislation. **The Company** should there- fore 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), Romanian Federal Act on Combating Money Laundering and Terrorism dated 10th October 1997 (AMLA) and the obligations and principles of the 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, S.R.L.** 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 into conflict with these, except for those that establish stricter conduct code and/or prevention measures.

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 about the prevention of 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 dated 26th 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 dated 1st August 2006** laying down implementing measures for Directive 2005/60/EC of the European Parliament and of the Council with regards to 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.

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 Romanian 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 dated 26th 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 foregoing points."*

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

The International Monetary Fund considers 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 trans- actions. 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 may 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 follows:

"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 an 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 dated 26th October 2005 regarding the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, describes 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 13th June 2002 on combating terrorism".*

Registered Office: Sat Hinchiriș, Comuna Lazuri de Beiuș, Nr. 126A, Judet Bihor.

Register Number: B-3457082

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

Contact:

Email: support@lescovex.com

Phone number: +41 78 726 14 31

Regardless of the fact that there is no official definition of customer in the aforementioned regulatory bodies, to the effect of this Manual we consider by "Customer" the following: *"any person, natural or legal entity, who has successfully passed 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 the 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 involvement in criminal activities or which are included in any public list concerning 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 their business make it impossible to verify its legitimacy or the source of its funds, or those whose 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 has been manipulated;

4. Legal entities whose shareholders or control structure cannot be determined;

5. Casinos, gambling/betting establishments, exchange offices, money transmitters and other similar entities that are not officially authorized;

6. Financial institutions resident in countries or territories without being physically present there (also referred to as "shell banks") and which do not belong to a regulated financial group.

On the other hand, the following persons, whether individuals or legal entities, shall only be accepted as customers by **The Company** with prior authorization from the Compliance Officer of **The Company**:

1. Customers involved in the production or distribution of weapons or other military equipment;

2. Duly authorized casinos, 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 "PEPs").

B. Risk Factors

For Money-laundering and Terrorism financing, **The Company** shall take into account various risk factors when evaluating and verifying the information and documentation provided by customers and, depending on these, Lescovex shall classify its customers as Low, Medium or High Risk Customers. The risk factors are, amongst others:

1. Geographic location: There are certain geographic locations considered as having a 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 or groups of similar nature; and those countries subject to sanctions by the aforementioned groups for not being compliant, or for 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 to say: a) Those who hold property, residence, offices or headquarters in a high risk country; b) Companies which have the majority of shareholders or beneficiary owners located in such countries; c) Any other substantial connections/links that might be identified.

Although Nationality is an important element it is not a determining factor for classifying 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 as high risk are as follows: Casinos, Gaming Centers, Racetracks; Financial Investment Corporations (S.A.F.I.); Arms, weapons manufacturers, distributors and dealers; Precious metals distributors and dealers; Professionals who act as intermediaries (lawyers or accountants that manage their customers' funds in their accounts); etc.

Clients may be considered High Risk Customers if possessing significant connections to activities considered to be high risk. The Compliance Officer will have to determine whether the connection is significant or not. There is always a significant connection if the firm is involved in or if a large portion of the firm's turnover comes from high risk activities.

1. **Politically Exposed Persons (PEPs)**: Public corruption is considered to be a 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 to them (such as family members or close associates) might pose a legal or reputational risk to our Company. Politically Exposed Persons (PEPs), as defined in 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, andsenior 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 Romanian 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 or close associates, or companies controlled directly or indirectly by PEPs, represents risks to the reputation of **The Company** similar to the 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 pay attention to the volume or amount of transactions channeled through the **Lescovex** platform, the source of the funds and the funds in their financial status. A limit to the funding will also be set in order to control those transactions, above which customers must obtain an authorization.

4. **Legal Entities:** Relationships 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 get information about the **beneficiary owners** of the legal entity, the type of operations related to **The Company**, the purpose of using the **Lescovex** platform, the source of the funds channeled through **Lescovex**, etc.

Beneficial owners are considered to be 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.

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

B. Customer identity verification

The Company considers that the most effective means of preventing the use of our services for 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 risks, such as Politically Exposed Persons (PEPs), irrespective of whether they are established customers or otherwise.

KYC and all due diligence procedures followed are not merely formal requirements that can be met by simply filling out a form. Nor is it a passive transaction whereby **The Company** simply requests information and documentation and the Customer provides everything. Instead, it is a dynamic, ongoing process through which **The Company** requests information, screens it to make sure it is complete and then requests supporting documentation when it is appropriate 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 various KYC procedures:

a) Paper-based verification:

This is the most 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).

b) Blockchain Certification Authority (BCA):

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

BCA integrates a method to add trusted certification entities (e.g. 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 belong to the public domain, it is not necessary to trust the entity responsible for managing the contract. Anyone can query fingerprints vetted by a 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 to attest whether entities have performed the appropriate controls necessary to authenticate the identity of any corporation or individual.

c) Video Identification:

Apart from the foregoing, in both cases **Lescovex** will carry out audiovisual 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 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, a facial recognition application called "Open Computer Vision" will be used, which allows to take snap shots. The communication will be conducted either through Skype or the Google Hangout application.

Before starting with the aforesaid procedure, **The Company** will have to obtain explicit consent from the customer to carry out this communication process, record it and take photographs mean- while. If the consent is not obtained, the customer may ask to go through a conventional identification procedure, by which he or she will have to send an authenticated copy of an identification document by postal delivery or other equivalent methods.

B. 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.zironex.io** and provide all the information and documentation required. Those steps are as follows:

1. Sing up on the website **www.zironex.io**: Customers will be asked to introduce a valid email address and password. Then a message will 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 email account is validated, customers will have to create a **Zironex** account, either a "Personal Account" or a "Corporate Account":

A) **PERSONAL ACOUNT**: Customers must verify their identity by following the paper-based procedure or by signing the KYC form with the BCA desktop application. In the former case, customers

must fill in 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 citizens, residents or tax payers of the USA, etc.

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

In addition, customers must upload a color copy of their ID or Passport together 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 that the date of issue, date of expiration and date of birth of the customer can be read easily. Expired or deteriorated copies shall not be accepted.

They must also upload a bank statement, tax bill, utility bill or any other such document, as a proof of residence. The address shown on this document must be the same as the one indicated in the form filled out or in the BCA signature.

Finally, aside from the foregoing, identification will be channeled via audiovisual real-time (live transmission) communication between the customer and **The Company**. This audiovisual interview will be made using Skype or the Google Hangout application. Explicit consent must be obtained from the customer before starting the video interview so as to conduct this audiovisual identification, to record it and to take photos during the process.

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

Customers may ask for any other conventional channel in order 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 categories set forth before, **The Company** may enhance the due diligence by asking for more information or documentation in order to decide whether or not to admit them as customers.

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

1) Firm's name;

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

3) Firm'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 or goods sold;

(ii) Depositing or withdrawing funds to business accounts;

(iii) Managing funds of other individuals;

(iv) Any other business activities (must be specified).

As in the foregoing case, when users verify their identity through the BCA procedure, they must also fill out the KYC form in order to provide the information that is not obtained through 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 corporate customer. This documentation could be sent by postal delivery, provided it is the original documentation, or by email, provided it is signed with a qualified electronic certificate pursuant to the Federal law on certification services in the area of electronic signature dated 19th December 2003:

- Powers of attorney of the person who is acting on behalf of the corporate customer during the creation process of the corporate account. If it is the firm's director, a notarized document of the appointment must be provided;

- Attestation of the entry in the appropriate register (normally, the Commerce Register);

- Memorandum of Association and Corporate bylaws or articles of association;

- Copy of the taxpayer register;

- Statement of the director or the board of directors' agreement by which it is expressly declared

that there is the will to acquire LCX token from **Lescovex**. A copy of the ID (front and back) or passport must be attached to this statement.

- Affidavit stating the following:

- Business activity and services provided;
- Typical customer profile;
- Type of payment systems accepted and the price of the services;
- Specification of the purposes of opening an account in **Lescovex** and using its services;
- The type of trading that is going to be carried out on the **Lescovex** platform;
- Identification of the shareholders, primarily the beneficial owners, considering them to be 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 first and last names; address; postal code; ID –front and back– or pass- port number; Readable copy of the ID or Passport).
- Identification of the firm's Directors (full first and last names; address; postal code; ID or passport number; Readable copy of the ID or Passport);
- Source of the firm's funds;
- Name, address and SWIFT code of the legal entity's bank;
- If the business is AML regulated, the policy must be stated, as well as how the firm performs KYC for the customers and any other due diligence measure. Additionally, AML and CFT Policy must be provided;
- 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);
- Declaration, if applicable, that the firm has another account in other cryptocurrency exchanges;
- How users can normally reach the services provided;

Depending on the characteristics of the firm and any other circumstances, **Lescovex** may enhance the due diligence and ask for any other information and documentation which is different to what has been set out before.

Apart from the foregoing, audiovisual 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 corporate customer.

B. Funding Limits

Individuals who have verified their accounts following the aforesaid procedure will be allowed to carry out deposit and/or withdrawals under the following limits, above which they will have to get in touch with **Lescovex**'s support staff (support@zironex.io):

	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 verified companies, they will be allowed to carry out deposits or withdrawals with the following limits, above which they will have to get in touch 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, if **Lescovex** identifies any suspicious transactions, it will ask the customer for more information or documentation, and if necessary, a report will be filed with the Reporting Office.

For both personal and corporate accounts the deposits and withdrawals of Fiat will only be allowed from and to their own bank accounts, and never to third party accounts.

C. Sanctions List Screening

The documentation and information provided by the customers will be verified and evaluated by **The Company**, namely by the Compliance Officer. Customers who have one or several risk factors and those who the Compliance Officer considers to do so, will have to provide more documentation and information so that the Compliance Officer can decide whether or not to accept them as customers.

Before deciding about whether or not a customer should be accepted, and in order to comply with the customer acceptance policy stated in this section, the Compliance Officer will check all persons,

natural or legal entities, using the watchlists. If a customer is found to be on one of the watchlists, all ties of that potential customer with **The Company** will be terminated and a report to the Reporting Office in Romania will be issued. If any potential customer is included in the PEPs list, the Compliance Officer's approval will be necessary.

D. Updating information and documentation

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

A 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 transactions will be carried out with the customer if their identification information is pending or out of date.

I. Follow-up regarding the Relationship with the customer

The type of transactions the customer conducts or requests as well as the amounts involved in such transactions should always be controlled to make sure that 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 transactions are carried out.

A. Definition of Suspicious Transactions

"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 forth in the previous section, **Lescovex** will carefully examine all the operations and transactions channeled through the platform in order to detect any unusual or suspicious transactions. To determine what is unusual or suspicious about a transaction, **Lescovex** will mainly pay attention to the trans- actions which show a lack of correspondence with the volume of activity or previous operational records of the customer, provided that there is no economic, financial, business or legal purpose for carrying them out, 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 on the **Lescovex** platform. It will solely permit deposits or withdrawals of Fiat that are made with the customer's bank account. If several people own the bank account, these others will have to be identified and will have to follow the KYC procedure, so that **The Company** can know at any time who they are and screen them on any sanctions list.

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

The Company has established various mechanisms inside its system in order to identify these transactions. Thus, all the addresses to which the money is sent are screened at any time using blacklists so that **Lescovex** can verify if it is related to any illegal activities. **The Company** has also fixed daily and monthly transaction amount limits, above which an authorization is needed to carry out transactions. Even the ones which are within the authorized range are at all time controlled by the system, so that it is always possible to check and verify any suspicious transactions made on the **Lescovex** platform.

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

The Committee, namely the Compliance Officer, will investigate the documentation related to the reported transaction. The analysis will be carried out as quickly and in depth as possible. After this investigation, the Compliance Officer will submit the results to the Committee, which will have the final say on whether or not to communicate the transaction to the Reporting Office. If so, all the documentation and details related to the suspicious transaction will be filed with the Reporting Office as set out in the next section. Otherwise, the incidence will be archived in **The Company** data- base.

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

In compliance with the applicable regulations, it is totally forbidden to disclose either the communications or the identity of the caller. As such, all this will be 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 the 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

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 information that will be relevant for evaluation. And also the reference to other files that could be related by inspecting the same individuals etc.

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

a) Analysis:

1. The documentation and information of the customer will be analyzed. The history of operations performed by the customer will be reviewed in the **The Company**'s register of operations 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 contact the customer directly in order to request additional information or documentation that is required according to each case. The Compliance Officer can also address the person who reported the operation.

3. In the event that a lack of clear correspondence is detected, the accreditation of the lawful origin of the funds must be requested.

a) Analysis outcome:

After in-depth investigation, the Compliance Officer will submit the research results to the Committee, which will then decide whether or not to communicate the incident to the Reporting Office. If the answer is affirmative, the operation will be communicated by the Compliance Officer, enclosing the documentation that supports the research carried out. Otherwise, the incident and all the details related to it shall be archived in the database of **The Company**.

A. Suspicious Transactions Report (STR) to the Money Laundering Reporting Office of Romania (Reporting Office)

If the Committee deems that there is enough evidence to consider that a transaction or operation has been made as part of an activity related to Money Laundering, Terrorism Financing or Fraud, the Compliance Officer will file a report with the Reporting Office in a timely form and manner. Cases in which **The Company** has terminated a relationship with a customer due to the reasonable suspicion of the customer being involved in such activities shall also be reported, just like when a customer has not been accepted for registration due to some of the Official Sanction Lists.

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

B. Confidentiality

Lescovex will not disclose the fact that information has been sent to or requested by the Reporting Office to any person involved or connected to the suspicious transaction or operation reported or to any third party. No reference whatsoever to the case will be made.

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

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

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, the 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, which shall be kept for a minimum of 10 years after the completion of the transaction or operation carried out;

3. Any Report of Suspicious Transactions issued and the documentation and information attached to it, which shall be kept during the 10 years following the date of the report.

Lescovex has its own database in which all this documentation and information will be stored so as to guarantee the due conservation and retrievability for both internal control and petitions from authorities. Once a person applies to be a **Lescovex** customer, the information and documentation will be registered in the **Lescovex** database, where it will be stored on an encrypted hard drive solely accessible by **Lescovex** through an internal VPN.

Lescovex believes that one of the best tools to combat money laundering and terrorism 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 the Prevention of Money Laundering and Terrorism Financing will be part of the internal procedures of **The Company** and knowledge and compliance will be mandatory for all those who are a part of it.

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

If there are any legal or regulatory modifications or improvements with regards to the Prevention of Money Laundering, Terrorism Financing or Fraud, the entire staff will be informed so that the new implementations can be applied and complied with properly.

Courses aimed at informing and training **The Company**'s staff to learn about the policy and how to apply the procedures related to the Prevention of Money Laundering and Terrorism Financing at **Lescovex** will be periodically provided for the staff by **The Company**.

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

1. Two members of the Board of Directors;

2. The Compliance Officer: the person, natural or legal entity, that may be a member of the Board of Directors or any other one hired to carry out the tasks related to this.

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

A. The Committee for the Prevention of Money Laundering and Terrorism Financing

The Committee will work as a collegiate body responsible for planning, coordinating and safe-guarding the compliance of the legal framework and the policies established in the Manual for the 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 its duties.

The Committee will meet at least every three months and will 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 specific issue related to it must be dealt with urgently, the Compliance Officer will convene an extraordinary meeting of the Committee.

The Committee will have, amongst others, the following duties and responsibilities:

- To draft the Manual for the Prevention of Money Laundering and Terrorist Financing to be approved by the Board of Directors;
- To report annually (through the Compliance Officer) to the Board of Directors regarding compliance with The Manual and all of **The Company**'s internal regulations related to the Prevention of Money Laundering and Terrorist Financing, suggesting, if needed, any pertinent modification to improve them or to implement any legal modifications, justifying the reasons and the manner in which this shall be done;
- To spread among the staff of **The Company** the information and documentation necessary in terms of Prevention;
- To design the training staff plan and its implementation;
- To 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;
- To decide on enhancements to the monitoring and control measures suggested by the Compliance Officer regarding the prevention of money laundering;
- To analyze the "Internal Operations Reports" submitted by **The Company**'s staff and approve or dismiss relaying suspicious transactions to the Reporting Office;
- To cooperate with the Reporting Office so as to provide all the documentation and information required;
- To preserve all the documentation and information generated by all the transactions and operations reported, as set out in Section VII of this Manual.

B. Compliance Officer

This position will 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 communicated to the FINMA and the Reporting Office (detailing name, position and branch). If there are any changes or updates in this information, the FINMA and the Reporting Office must also be notified, within 5 days after the Officer's appointment.

The Compliance Officer will have, amongst others, the following responsibilities and duties:

- To convene the meetings of the Committee;
- To 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;
- To receive the petitions from the Reporting Office to provide information and documentation and to execute the actions asked for;
- To implement the Manual;
- To monitor transactions carried out by customers;
- To investigate reports of unusual transactions, as well as those detected in the centralized monitoring process;
- To keep the rest of the committee members informed of any circumstances that could alter the prevention policy contained herein;
- To present before the Committee suggestions to improve or implement new procedures for The Manual;
- To keep **Lescovex** informed and updated about any legal matters and regulations that affect **The Company** in its management of the prevention against money laundering.

Due to the nature of the services provided by **Lescovex**, **The Company** will apply various methods to guarantee the security of the transactions and to avoid that the platform be used as a 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 as to prevent transactions related to money laundering and terrorism financing. These policies and procedures, some of which have been set out in this Manual, will be circulated among all the employees and executives of **The Company**.

The aforementioned policies will include a description of the 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 for each case. As has been said, the customer must provide all the information and documentation required so that **The Company** is able to verify the customer's identity and establish a profile for each of its customers. If any of them has any of the risk factors mentioned, **The Company** will enhance the due diligence by asking for more information or documentation to decide whether or not to accept a person as a **Lescovex** customer.

On the other hand, and in order to control the transactions made by customers, **Lescovex** will pay attention to the transactions carried out by customers and its correspondance with the profile which has been established for each customer. If the system detects that any of the transactions made do 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 in order to initiate an

investigation. To this effect, **The Company** has also established a daily and monthly amount for trans- actions, to deposit or withdraw cryptocurrencies or legal tender, above which an authorization must be granted by **The Company**, so as to keep all transactions under control.

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

The Company will always verify that the bank account to or from which the customer deposits or withdraws legal tender is owned by the customer and nobody else. If any other person is a co-owner, **Lescovex** will also ask for information and documentation related to that co-owner, in order to have the necessary information so as to know at all times 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 that it is guaranteed that the transaction has been made only by them. Apart form that, an email will be sent to their email account to verify if they have made that transaction.

The Committee will be in charge of applying and developing this Manual and all the regulation and policies related to the Prevention of Money Laundering and Terrorism Financing, keeping the afore- mentioned Manual updated at all times and avail- able for the relevant authorities.

The most important commitment by **Lescovex** is the compliance with all that has been set forth in this Manual and any other regulations and policies related to the Prevention of Money Laundering and Terrorism Financing. This way, apart form the internal control measures already established, **Lescovex** will be audited by external audit entities, so that there is verification that the procedures to prevent money laundering and terrorism financing which have 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 have 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 aforementioned report will be available to any authority during the following five years after being issued.

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**'s written permission, and contents thereof must not be imparted to a third party nor be used for any unauthorized purpose.