IAESIR FINANCE

IAESIR Finance
www.iaesirfinance.com

IAESIR

IAESIR Finance Regulatory Compliance Manual

Operations Manual and Code of Ethics

Compliance Office

@iaesirfinance @iaesirfinance support@iaesirfinance.com

IAESIR FINANCE

MANUAL OF INTERNAL POLICIES FOR THE PREVENTION OF MONEY LAUNDERING AND THE FINANCING OF TERRORISM

INTRODUCTION

COMPLIANCE OFFICE

From the General Directorate and all the members who make up the IAESIR team, we are aware of the importance that the prevention of money laundering and the financing of terrorism raises.

The Company has approved this Manual for the Prevention of Money Laundering and Financing of Terrorism (PBCFT), which in addition to being supervised for compliance by our internal Compliance department, has an external audit by our partner in Compliance RAP Informes Legales SL, as well as with express validation by our official BINANCE Exchange.

In order to continue complying with the obligations provided for in the PBCFT regulations, and transparency in all our procedures being our main maxim to follow, we make this manual available to you to serve as a help and reference when it comes to knowing our way of operating and the procedures to follow to guarantee maximum safety for our clients.

TITLE I. INTERNAL DUE DILIGENCE PROCEDURES, CUSTOMER ADMISSION AND OPERATION ANALYSIS

Article 1.- Due diligence measures

1.1. CUSTOMER ACCEPTANCE

As a development of the provisions of the Manual, the customer acceptance procedures, as well asYoas well as the identification and knowledge procedures, help protect the Company from being used as a vehicle to carry out criminal activities or to defraud the entity itself.

The procedures are therefore intended to prevent risks (reputational, operational, legal...) that may involve the Company in participating, even involuntarily, in illegal or unethical activities.

The acceptance of clients by the Company is based on the establishment of commercial relationships based on transparent communication and the client himself being the one to affirm or deny his own information and on knowledge of the investee companies and their economic activities.

It should be noted that the Company does not recommend any type of investment or promote or encourage the carrying out of any type of operation.Yonor does it favor or recommend that investment decisions be made based on the investment recommendations made by the Company.

The Company will classify clients in accordance with the classification detailed below, limiting its operations to the preconceived risk depending on the section where it operates, taking into account that the operations carried out by the client are totally autonomous and designed by the client themselves. limiting the Company's responsibility to proving the origin of the funds each time it requests entry as a client.Yoas its economic capacity is sufficient to be able to assume the risk in the operation it poses. These limits are based on the Company's internal risk orientation that is approved by the administrative body, periodically, asYoas implemented and developed internally.

Identification and knowledge of clients
When establishing commercial relationships, the Company requires identification through biometric testing and proof of life of its clients.

It is important to highlight that commercial relations will not be initiated when the client refuses to identify themselves or the identification is not truthful or sufficient.

Verification of the identity of potential clients will be carried out using current reliable documents, with a photograph and signature, verifying that the signature used in the contracts and receipts matches that of the identification document.

The clear and concrete identification of the client is an essential element within the process of establishing relationships, así ć oas obtaining all the necessary information about the identity of each new client.

The identification process is articulated as follows:

- · Documentation for identification and knowledge of the client: In the Company's client acceptance procedure, the necessary information and documentation will be requested in accordance with current internal regulations:

- · Identification of the natural or legal person: Residence Card, Foreigner Identity Card or valid Passport / CIF of the company and deed of incorporation. In the case of non-resident legal entities, they musttoSecure the Hague Apostille if necessary.
- · Deed of powers under which the representatives and authorized persons operate.
- · Identity document of the people who act as authorized/representatives.
- · Writing of powers of representatives and authorized persons.
- · The ownership or control structure must be determined, providing a descriptive document of the shareholding structure, duly signed by the administrator.
- · Responsible declaration from the client as the ultimate beneficiary to identify the beneficial owner (natural person) or certificate of beneficial ownership from the notary and, for companies with higher than average risk, verification of said identification by obtaining documentation or reliable external sources.
- · Documentation that certifies the economic or professional activity indicated by the company.
- · In cases of subjects obliged to the Law on the Prevention of Money Laundering and the Financing of Terrorism, accreditation of their condition and/or audit by an external expert.
- · Public information to evaluate possible reputational risks.

All the identification and knowledge of the client documentation collected is digitized and filed in the client's file folder.

Identification of the Real Owner:

Prior to establishing business relationships or executing any operation, the necessary measures must be identified and adopted to verify the identity of the Beneficial Owner.

For the purposes of the Law, the Real Owner is understood to be:

1. The person or natural persons on whose behalf it is intended to establish a business relationship or intervene in any operations.

2. The person or natural persons who ultimately own or control, directly or indirectly, a percentage greater than 25% of the capital or voting rights of a legal entity, or who through agreements or statutory provisions or otherwise means exercise control, direct or indirect, of a legal entity.

They will be control indicators by other means, among others, those provided for in Article 22 (1) to (5) of Directive 2013/34/EU of the European Parliament and of the Council of 26 June 2013 on annual financial statements , the consolidated financial statements and other related reports of certain types of companies.

Exceptions are companies that are listed on a regulated market and are subject to information requirements in accordance with Union Law or equivalent international standards that guarantee adequate transparency of ownership information.

If there is no natural person who has a percentage greater than 25%, the administrator or administrators will be considered to exercise said control. In the event that the administrator is a legal entity, it will be understoodtothat control is exercised by the natural person appointed by the legal entity administrator.

3. The person or natural persons who own or exercise control of 25% or more of the assets of a legal instrument or person that manages or distributes funds, or, when the beneficiaries have yet to be designated, the category of persons for the benefit of which the legal person or instrument has been created or primarily acts.

Information must be collected from clients to determine whether they are acting on their own behalf or on behalf of third parties. When there are indications or certainty that the clients are not acting on their own account, the precise information must be collected in order to know the identity of the people on whose behalf they are acting and, if they are people classified as having a risk higher than average, obtain and digitize the identification documentation of the beneficial owners, the documentation that proves their economic or professional activity and the documentation that proves the consistency of the lawful origin of the funds they contribute, as indicated in the previous chapter.

Appropriate measures must be adopted to determine the ownership and control structure of legal entities.

The Law requires not to establish or maintain business relationships with legal entities whose ownership and control structure has not been determined. In the case of companies whose shares are represented by bearer securities, the previous prohibition will apply unless the ownership and control structure can be determined by other means. This prohibition will not betoApplicable to the conversion of bearer securities into registered securities or account entries.

It is duetoinform about the shareholding or control structure of all legal entities already registered previously, since they cannot be linked as owners or equivalents to any new contract or product in the event that such information does not exist. The Link Detail Screen Allowtoalso access the shareholding or control structure form to complete the information and be able to finalize the link.

In addition to what is described in the preceding letters, in the event that the legal entity is classified by the system as high risk in terms of PBCFT, it musttorecord in the “shareholding or control structure” document, if it exists, the entire chain of legal entities introduced until the natural persons who are the real owners are identified, obtaining documentation that proves the ownership of all of them.

However, betoObtaining additional documentation or information from reliable independent sources is mandatory when the client, the beneficial owner, the business relationship or the operation presents higher than average risks, así ćomo:

to. When there are indications that the identity of the beneficial owner, declared by the client, is not exact or truthful.

b. When there is evidence of money laundering or terrorist financing that requires special examination or communication based on evidence.

A digital identity test is carried out through a digital verification system in which, in addition to inserting photographs, a scan of all supporting documentation will be requested.

Both the photographs and the scanned documentation will become part of the IAESIR digital archive, which complies with all legal measures for compliance with the Data Protection Law.

1.2. PROHIBITED PEOPLE

Commercial relationships will not be established or maintained with people who make it difficult, through concealment or by any other means, to provide data on their identification, personality, residence or activity. Nor will commercial relations be established

with people who are known to be related to any criminal activity, nor with natural or legal persons that operate without the pertinent administrative authorizations in cases where they are necessary.

To do this, the appearance of the potential client is checked against the international lists that we have internally configured during their admission.

Therefore, when in the previous contacts with the potential client, the reasons why they intend to open the account do not seem clear, or when they cause doubts or reasonable suspicions about the legality and coherence of the activities they carry out or operations that they intend to channel. , the person will be informed that we cannot attend to their request to start commercial relations.

AceYoTherefore, business relationships will not be established with the following categories of clients or suppliers:

- Persons or entities linked to terrorist groups or organizations or those that carry out terrorist activities or contribute to the purposes pursued by said groups or organizations, as well asYonor are those persons or entities included in any of the public lists of persons sanctioned for links to terrorism or related groups.

- Persons or companies that are known to be related to any type of criminal activity. Persons or companies that have
- businesses whose nature makes it impossible to verify the legitimacy of their activities or the origin of their funds.

- Persons or companies that refuse to provide information or the required documentation.

- Any natural person, entity or organization that legally must have some administrative authorization to operate, and that lacks it (investment companies, payment entities, money remitters, casinos, bingo halls, NGOs, exchange houses, etc.).

- Activities related to the provision of sexual services (brothels, hostess clubs, etc.). Associations or similar related to the
- consumption of narcotic or similar substances (marijuana smoking clubs, etc.).

- Target persons who were subject to special examination and determinedeitherits cancellation, and that in the new registration request there are indications of BCFT or the information or documentation provided is insufficient to apply the enhanced due diligence measures.

1.3. SEGMENTATION BY CUSTOMER RISK

In this sense, the Company has categorized clients into three classes:

a) Unqualified retail clients: This is the category in which the majority of individual investors fall. Their trading limit is lower given that they are those with less knowledge and experience in purchasing or operating this type of asset. As a retail client, you will receive the highest degree of protection.

b) Advanced retail clients: They will be those who claim to be such or due to their way of acting it is detected that they have that condition. Its operating limit is higher and more documentation is required. As a result, they receive less protection as they are better able to understand the nature and risks of investment markets, products and services.

c) Professional clients: those who operate on behalf of third parties.

1.4. APPLICATION OF DUE DILIGENCE MEASURES IN ACCEPTING NEW CUSTOMERS

The Company will request completion of the “Know your client” questionnaire in which the client agrees to tell the truth.

You will be provided with a document based on the type of client that you indicate with questions appropriate to the type of client for which you are going to classify.

In addition to the above, the Company will carry out the following operations:

- Tracking of all the people involved in the operation. Before starting the business relationship, the people involved must be manually compared.
- Analysis of the information/documentation provided: The Company will request the necessary documentation to know the ownership structure, the beneficial owners, the resulting shareholding after the investment or divestment operation, as well as the company's administrative body.
- The analysis of the information provided will take into account:
  - Coherence of the information and documentation provided.
  - Carrying out the necessary and reasonable controls to verify the veracity of the information provided (through additional mechanisms such as official records, Web pages, economic information services or others that at any given time are more appropriate to verify the information).
  - Verification of the company's operations/linkages with high-risk countries in terms of money laundering and/or terrorist financing.

As Clients address the Company through telematic means, without being physically present, in order to establish business relationships, one of the following circumstances must occur:

a) The identity of the Client is accredited in accordance with the provisions of the applicable regulations on electronic signature, by means of a qualified electronic signature.

b) The identity of the Client is proven by a copy of the Residence Card, Foreigner Identity Card or valid Passport.

c) The first deposit comes from an account in the name of the same Client opened in an entity domiciled in the European Union or in equivalent third countries.

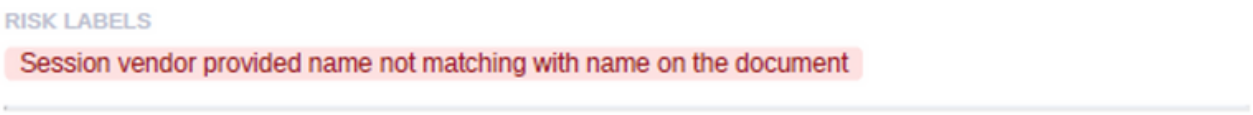
d) The identity of the client is proven through the use of other secure client identification procedures in non-face-to-face operations, provided that such procedures have been previously authorized by the Prevention Agency.

In any case, within a period of one month from the establishment of the business relationship, a copy of the documents necessary to carry out due diligence must be obtained from these clients.

When discrepancies are noted between the data provided by the client and other accessible information, it will be mandatory to contact the Client.

As previously stated, in the business relationships maintained by the Company, which are non-face-to-face, the enhanced due diligence measures indicated above will be applied.

The application used will execute the following analysis control of the documentation provided automatically, warning if it does not match the data provided, as shown below



In case of doubt or suspicion, an immediate escalation occurs that analyzes the documentation provided.

Any person who, due to their profession or activity, belongs to the General Administration of the State, Administrations of the Regions, Entities that make up the local administration as well as any other entity in the public sector or is an Authority, that is, any person who has a position or own jurisdiction as a member of any corporation, court or collegiate body, and in any case if

belongs to the Congress of Deputies, the legislative Assemblies or is an elected official of a political party (hereinafter “PRP”) will be treated as an advanced retail client for the purposes of providing documentation.

1.5. CONTINUOUS MONITORING OF THE BUSINESS RELATIONSHIP

The Company will apply continuous monitoring measures to the business relationship throughout said relationship in order to guarantee that:

a) The information provided by the Client coincides with the knowledge we have of the Client and its business and risk profile, including the origin of the funds.

b) The documents, data and information available are up to date. The update will be mandatory when a relevant change is verified in the client's activity that could influence their risk profile.

1.6. REVIEW OF DOCUMENTATION AND INFORMATION

The Company will review all documents, data and information obtained as a result of the application of the due diligence measures described in this Manual, to guarantee that they are kept updated and current and a communication will be made to the designated person responsible for money laundering if it is detected. some suspicious behavior.

Notwithstanding the above, all documentation and information relating to a Client will be immediately updated when there is knowledge of a relevant change in the Client's activity that could influence its risk profile.

Article 2.- Conservation of documents

The Company will keep the originals or copies with evidentiary force of the corresponding documents or records that adequately prove the performance of operations and business relationships with its Clients for ten years.

For a period of five years, the Company will keep a copy of the reliable identification documents, the client's statements, the documentation and information provided by the client or obtained from reliable independent sources, the contractual documentation, and the results of any analysis carried out.

The reliable identification documents of the parties involved in a business relationship or an operation will be stored on optical, magnetic or electronic media that guarantee their integrity, the correct reading of the data, the impossibility of manipulation and their adequate conservation and location.

Likewise, the Company will keep information on those operations that were merely attempted that were not executed taking into account their associated risk in order to communicate them to the Prevention Body if necessary.

Once the period of ten or five years has elapsed, in accordance with the above, the documentation will be eliminated.

Article 3.- Simplified due diligence measures

The Company, depending on the risk and depending on the type of Client, will apply simplified due diligence measures with respect to the following Clients:

a) Public law entities of the Member States of the European Union or equivalent third countries.

b) Companies or other legal entities controlled or majority owned by public law entities of the Member States of the European Union or equivalent third countries.

c) Financial entities, except payment entities, domiciled in the European Union or in equivalent third countries that are subject to supervision to guarantee compliance with obligations to prevent money laundering and the financing of terrorism.

d) Branches or subsidiaries of financial institutions, except payment institutions, domiciled in the European Union or in equivalent third countries, when they are subject by the parent company to procedures for the prevention of money laundering and the financing of terrorism.

e) Listed companies whose securities are admitted to trading on a regulated market in the European Union or equivalent third countries, as well as their majority-owned branches and subsidiaries.

In the preceding cases, the Company may apply, depending on the risk, one or more of the following measures:

a) Verify the identity of the Client or the beneficial owner only when a quantitative threshold greater than 100,000 euros is exceeded, after the establishment of the business relationship.

b) Reduce the periodicity of documentary review, so that it becomes two (2) years.

c) Do not collect information about the Client's professional or business activity, inferring the purpose and nature from the type of operations or business relationship established.

The application of simplified due diligence measures is prohibited in the case of third countries not classified as equivalent or in respect of which the European Commission adopts a sanctioning decision.

In any case, the Company will gather sufficient information to determine whether the Client can benefit from one of the exceptions provided for in this article.

Under no circumstances may the Company apply simplified due diligence measures, or will it cease to apply them, if indications or certainty of money laundering or terrorist financing or above-average risks occur or arise.

Article 4.- Reinforced due diligence measures.

In addition to the normal due diligence measures, the Company will present enhanced measures in relation to countries that present strategic deficiencies in their anti-money laundering and anti-terrorist financing systems and appear in the decision of the European Commission adopted in accordance with the provisions of article 9 of Directive (EU) 2015/849 of the European Parliament and of the Council, of May 20, 2015.

Likewise, in addition to the normal due diligence measures, other reinforced measures will be applied on occasions when the special nature of the business presents a higher risk of money laundering or terrorist financing, which will be applied in any case in the following activities :

a) Operations in unusual circumstances (those whose amount, characteristics and periodicity are not related to the client's activity and type, are outside the parameters of normality or do not have an obvious legal basis).

b) Operations with non-resident clients in the European Union.

c) Operations with companies that merely hold assets.

d) Operations with companies whose shareholding and control structure is not transparent or is unusual or excessively complex.

e) Operations with clients who regularly use bearer payment methods.

f) Operations with clients from risk countries, territories or jurisdictions included in this Manual, or that involve transfer of funds from or to such countries, territories or jurisdictions.

These measures will consist in any case of:

- Apply appropriate risk-based procedures to determine the risks associated with the operation.
- Update, at least annually, the data obtained in the customer acceptance process.
- Obtain additional documentation or information about the Client and the beneficial owner (e.g. tax returns, payrolls, contracts, public deeds, certificates from Public Registries, auditor reports, opinions of independent experts, ...)

Likewise, limitations may be imposed on the operations due to their nature, their amount or the means of payment used, such as those set out in the following Article, which may be terminated, depending on the presence of indications or certainty of a relationship in the operation. with money laundering or financing of terrorism, with its non-execution and with a communication to the Prevention Agency.

Article 5. Special examination of suspicious transactions

The Company will examine, within their respective spheres of action, any operation that by its nature may be apparently linked to money laundering or the financing of terrorism, that is, any operation that is complex, unusual, or that does not have an economic or lawful purpose. apparent, or that presents signs of simulation or fraud and, in particular, the operations described below. These operations may require actions regarding the acceptance or rejection of Clients, their classification based on money laundering risk criteria, the making of communications or special analysis of operations.

Below is a list of characteristics that, if present in an operation, may lead to it being considered suspicious:

- Due to the size and frequency of operations

a) Structuring transactions in small amounts, or in amounts below record-keeping or reporting thresholds, similar to structuring cash transactions.

b) Perform multiple high-value operations:

- In short succession, such as a 24-hour period;
- In a staggered and regular pattern, with no further operations recorded for a long period afterwards, which is particularly common in cases involving ransomware; either
- To a newly created or previously inactive account.

c) Transfer cryptocurrency immediately to multiple virtual currency exchange or virtual currency wallet service providers ("Provider"), especially providers registered or operating in another jurisdiction where:

- there is no relationship to where the customer lives or conducts business; or
- non-existent or weak PBCFT regulation.

d) Deposit a cryptocurrency into an exchange wallet and then, often immediately:

  - withdraw the cryptocurrency without exchange activity to other cryptocurrencies, which is an unnecessary step and incurs trading fees;
  - converting cryptocurrencies into multiple types of cryptocurrencies, again incurring additional trading fees, but without a logical business explanation (e.g. portfolio diversification); either

  - withdraw cryptocurrencies from a Lender immediately to a private wallet.

e) Accept resources suspected of being stolen or fraudulent:

· Deposit resources from wallet addresses that have been identified as holders of stolen funds, or wallet addresses linked to holders of stolen funds.

- Operations related to new users

a) Making a large initial deposit to open a new relationship with a Lender, while the amount financed is inconsistent with the client's profile.

b) Make a large initial deposit to open a new relationship with a Lender and fund the entire deposit on the first day it is opened, and have the customer begin negotiating the full amount or a large portion of the amount that same day or a day later , or if the client withdraws the full amount the next day. As most cryptocurrencies have a transactional limit for deposits, laundering large amounts can also be done through over-the-counter trading.

c) A new user attempts to trade the entire balance of the cryptocurrencies, or withdraws the cryptocurrencies and attempts to send the entire balance off the platform.

- Operations relating to all users

a) Operations that involve the use of multiple cryptocurrencies, or multiple accounts, without a logical commercial explanation.

b) Make frequent transfers in a given period of time (for example, a day, a week, a month, etc.) to the same cryptocurrency account:

- by more than one person;
- from the same IP address by one or more people; or in
- relation to large quantities.

c) Incoming transactions from many unrelated wallets in relatively small amounts (accumulation of resources) with subsequent transfer to another wallet or complete exchange for fiat currency. Such operations of several related cumulative accounts may initially use cryptocurrencies instead of fiat currency.

d) Perform a virtual-fiat currency exchange with a potential loss (for example, when the value of cryptocurrency fluctuates, or regardless of abnormally high commissions compared to industry standards, and especially when the operations have no explanation commercial logic).

e) Convert a large amount of fiat currency into cryptocurrency, or a large amount of one type of cryptocurrency into other types of cryptocurrency, without a logical business explanation.

When, in accordance with the above, an operation is being subject to special analysis, the analysis phases, the procedures carried out and the sources of information consulted must be documented, in accordance with the following protocol:

Each operation or suspicious fact detected will receive a file number to facilitate its organization and communications in reference to it.

The information and documentation obtained from the client, external public information sources (official records (commercial, property...), internet searches, in-person visits to offices, warehouses or premises declared by the client as places where they practice) will be analyzed. its commercial activity, and the history of operations carried out by the client previously in the Company's operations register will be reviewed in order to verify the correspondence between amounts, dates, beneficiaries, documents provided, frequency, concept...

If the information is incomplete or insufficient to draw a conclusion about the suspicious nature of the operation, the Controller will contact the client directly in order to obtain the additional information or documentation that is necessary in each case.

The correspondence between the client's activity and the operations carried out will be studied. In the event that a lack of clear correspondence is detected, accreditation of the funds must be requested.

The different databases to which the Company may have access will be used to find out if there is any coincidence between the names and surnames of the people on said lists and the names and surnames of the people involved in the suspicious operation.

If additional information is needed, you must contact the person who reported the operation.

Once the technical analysis is completed, the Compliance Officer will determine whether or not to communicate to the Prevention Agency, depending on the presence in the operation of indications or certainty of a relationship with money laundering or the financing of terrorism. Any decision by the person responsible for laundering must be based on homogeneous criteria and must be duly motivated.

Compliance Officer will be responsible for preparing, reviewing annually and disseminating via email among its managers, employees and external collaborators a

list of operations that, due to their nature, may be likely to be related to money laundering and the financing of terrorism.

Article 7.- Duty of confidentiality

The obligated entities will not reveal to the Client or third parties the actions they are carrying out in relation to their PBCFT obligations.

The internal communication procedures of the entities obliged to the Compliance Officer as well as the external communication procedures of the latter to the Prevention Body will respond to the principles of speed, security, effectiveness and coordination.

In particular, obliged entities must maintain the strictest confidentiality with respect to the operations that are being analyzed or have been communicated to the Prevention Agency.

Article 8.- Alerts and internal information. Communication of potential breaches

a) Communication of suspicious operation

The Company has established communication procedures so that facts that may be relevant to the PBCFT can be immediately communicated to the Compliance Officer.

The communications must contain at least the data that allows individualization of the affected subject or subjects, facts or operations, amounts, place and dates to which they are limited, as indicated in the form enabled for these purposes. These communications must be recorded both for the communicator and for the communication body.

Internal communications to the Compliance Officer will be made by email. Each employee will send it to the Compliance Officer at the address he has available or by personally delivering it in a sealed envelope.

Once communication has been made to the Compliance Officer, the manager or employee will be exempt from liability.

The Compliance Officer will adopt appropriate measures to maintain the confidentiality of the identity of the person/s who made the communication.

Once a communication is received, the Compliance Officer will proceed to immediately analyze or verify it to determine the relationship of the events or operations reported with money laundering. If there is evidence or certainty of money laundering, the proceeding will be as indicated in this Manual. Any operation identified as the object of necessary special analysis will appear in a sequential numerical record in which, in addition to said identification number, the following fields will appear:

a) Opening date of the analysis file.

b) Succinct description of the reason for including the transaction in the analysis.

c) Description of the analyzed operation.

d) Decision on the file and the reasons on which it is based.

e) Closing date.

f) Decision on whether or not to communicate it to the Prevention Agency and its date, as well as the date on which, if applicable, it was carried out.eitherthe communication.

g) Other data.

Transactions in which the circumstances under consideration in this procedure occur will be the subject of a physical file. It will include a copy of the documents associated with the analysis carried out.

The analysis techniques to be used, in accordance with the decision of the Compliance Officer, and, in any case, in accordance with the specific characteristics of the investigation in progress, will be the following:

a) Internet search.

b) Search in Official Records (depending on their existence, and according to the jurisdiction of the interveners).

c) Request for an opinion from the Client's manager.

d) Consultations with third parties.

e) Economic-financial analysis of transaction data (reconstruction of movements, analysis of cash flow sufficiency, quantification of the origin of funds, etc.).

f) Others that, according to the characteristics, could contribute to its clarification (interviews, additional requests for information from those involved, etc.).

Every analysis must conclude with one of the following decisions:

a) Communication to the Prevention Agency of the transaction because it is considered suspicious, in accordance with the appropriate rules for decision-making and the procedures in force for such resolution.

b) File the actions because the transaction is considered normal.

c) Maintenance of monitoring of the interveners until a degree of clarification is achieved that allows classification in one of the two previous states.

Whatever the criterion adopted, the Obligated Person will be informed of the course given to their communication.

Every employee has the possibility of directly communicating to the Prevention Agency operations with indications or certainty of being related to money laundering, in cases where the Compliance Officer does not inform the communicator of the course given to his communication within a period of twenty days. Skilled from communication to the Compliance Officer.

b) Communication of potential breaches

The Company has an internal complaints channel available to all its employees, directors or agents so that they can communicate, even anonymously, relevant information about possible non-compliance or shortcomings, in the area of PBCFT, that take place within the Company. both in relation to express non-compliance with the applicable regulations, and in the development of internal policies and procedures.

The channel will be managed by the Representative, who will exercise the functions of its administrator, processing the complaints received so that the corresponding resolutions are adopted.

The processing of complaints will be carried out in accordance with the regulations on the protection of personal data.

The complaints channel is established as an internal, independent channel with sufficient guarantees of confidentiality and protection of the complainant against possible retaliation, discrimination and any other type of unfair treatment.

The procedure does not require the identification of the complainant, although if this occurs, the channel administrator will guarantee confidentiality, provided that it is acted in good faith, throughout the process and, in particular, that the accused and, where appropriate, their superiors cannot access the identifying data of the complainant, unless this is strictly necessary for the resolution of the file.

The period available to the Compliance Officer to resolve the open procedure will be 15 calendar days, counting from the day after the administrator received the complaint. Within this period of time, the complainant may find out about the status of their complaint by sending an email to the administrator using the reference number that will appear on the initial acknowledgment of receipt, who must resolve it within 48 hours. The complainant must maintain confidentiality regarding the information of which he or she becomes aware within the framework of the procedure.

c) Alert System

The Company will determine an alert system through the application of computer tools in accordance with the provisions of article 16.

Article 9.- External communications to the Prevention Agency

9.1- Communication of suspicious operations

Once the special examination established in article 5 has been carried out, and having determined that the operation contains evidence or certainty of a relationship with money laundering or the financing of terrorism, the communication based on evidence will be carried out without delay, using, in its case, the form that the Prevention Agency may have enabled for these purposes.

Without prejudice to the foregoing, the Company will immediately adopt additional risk management and mitigation measures, which must take into account the risk of disclosure.

The communication of suspicious transactions will contain, in accordance with PBCFT regulations, the following information:

a) The relationship and identification of the natural or legal persons participating in the operation and the concept of their participation in it.

b) The known activity of the natural or legal persons participating in the operations and the correspondence between the activity and the operations carried out.

c) The list of the operations and dates to which they refer, indicating their nature, currency in which they are carried out, amount, place or places of execution, purpose and payment or collection instruments used.

d) The procedures carried out within the framework of the special examination regulated in this Manual.

e) Exposition of the circumstances of all kinds from which the indication or certainty of connection to "money laundering" can be inferred or that reveal the lack of economic, professional or business justification for carrying out the activities.

f) Information about the decision adopted or that will foreseeably be adopted regarding the continuation or interruption of the business relationship with the client or clients participating in the operation, as well as the justification for this decision.

Article 10.- Controls for the detection of the possible relationship of Clients with the financing of terrorism or PRP

a) EU List

The Company will consult the European Union list of sanctions and terrorist organizations and groups prior to the admission of a Client, in addition to the periodic cross-checking of said lists with existing Client databases when updates occur. This filter will be carried out by the Company Representative. This list (and modifications to it) can be found at the following internet addresses:

https://data.europa.eu/euodp/es/data/dataset/consolidated-list-of-persons-groups- and-entities-subject-to-eu-financial-sanctions/resource/3a1d5dd6-244e-4118- 82d3-db3be0554112

https://eeas.europa.eu/headquarters/headquartershomepage_en/8442/Consolidated%20list%20of%20sanctions

https://www.consilium.europa.eu/en/policies/fight-against-terrorism/terrorist-list/

The aforementioned contrast will be carried out with the following periodicity:

1. Possible new Clients: before being admitted through comparison in the internally accessible applications.

2. Clients already admitted: each time the list is updated or, where appropriate, on a semi-annual basis by the Company.

The Representative will leave a written record of the contrast. In case of positive results with the European Union list, the person will not be admitted as a Client.

b) PRP control

The Company will verify whether its Clients meet the definition of a person with public responsibility through the Client's declaration, as well as consulting third-party records. In the event that the Client meets the definition of a person of public responsibility, it will apply the pertinent measures, in accordance with the procedures described in this Manual.

TITLE II. OF EVALUATION PROCEDURES

Article 11.- Risk analysis

The Company's internal control procedures will be based on a prior risk analysis carried out by the Company. Specifically, the Company will prepare a Risk Self-Assessment Report of an eminently practical nature adapted to its activity, in which its exposure to the risk of money laundering and terrorist financing is identified and evaluated.

Specifically, the following aspects will be taken into account in the aforementioned self-assessment report:

a) Basic information about the Company.

b) The channels used for the entry, movement and transmission of funds, with reference to the risk they pose.

c) Types of clients, specifying those who may present a greater risk in terms of prevention.

d) Client actions that may pose a greater risk of money laundering and terrorist financing.

e) The purpose of the operation.

f) The level of the client's assets, the volume of operations and the regularity or duration of the business relationship.

g) Geographic areas of activity of the Company, specifying those with the highest risk with or in which the obligated entity operates.

The risk analysis will be reviewed by the Compliance Officer on an annual basis and, in any case, when a significant change is verified in the activity, business volume or structure of the Company that could influence its risk profile.

Article 12.- External Expert Report

The internal control and communication procedures and bodies will be subject to annual review by an external expert.

The independent expert's report must be issued within two months following the reference date. In any case, in the two years following the issuance of the report, it may be replaced by a monitoring report issued by the external expert, and referring exclusively to the adequacy of the measures adopted by the Company to resolve the deficiencies identified where appropriate. .

The results of the examination will be recorded in a confidential written report that will describe in detail the existing internal control measures, assess their operational effectiveness and propose, where appropriate, possible rectifications or improvements. This report, which will include a detailed description of the professional career of the expert who writes it, will be available to the Prevention Agency for the five years following the date of its issuance.

Suggestions for rectification or improvement, as well as the most significant conclusions of the report, must be brought to the attention of the administrative body within a maximum period of three months from the date of issue of the report, with a record of the taking into consideration in the minutes.

In the event that there are deficiencies, the administrative body will adopt, without delay, the necessary measures to resolve the deficiencies identified in the external expert reports. And if the deficiencies are not susceptible to immediate resolution, the administrative body will expressly adopt a remedy plan, which will establish a precise calendar for the implementation of corrective measures that may not exceed, in general, one calendar year.

The external examination may not be entrusted to those individuals who have provided or provide any other type of paid services to the Company during the three years before or after the issuance of the report.

All clients can check the validity of the External Compliance supervisions through the following links:

https://rapinformes.es/prevencion-blanqueo-capitales-finacion-terrorismo/

https://rapinformes.es/compliance-penal/

Likewise, there is a direct communication channel with our manager at Binance, Edgar Arellano Reyes, (edgar.r@binance.com), to whom you can consult any questions related to the management of IAESIR.

Article 13.- Ethical standards in the hiring of employees, managers and agents

The Company guarantees high ethical standards in the hiring of directors, employees or agents. For these purposes, the suitability criteria established by the sectoral regulations that apply to them at all times will be applied to these groups. In the absence of specific regulations, to determine the concurrence of high ethical standards in directors, employees or agents of the obligated subject, their professional career will be taken into consideration, assessing observance and respect for commercial or other laws that regulate economic activity. and business life, as well as good practices in the sector of activity in question.

In any case, it will not be considered that high ethical standards are met when the employee, manager or agent:

- · Have a criminal record that has not been canceled or susceptible to cancellation for intentional crimes against property, and against the socioeconomic order, against the Public Treasury and Social Security, crimes against the Public Administration and falsehoods;
- · Has been sanctioned by a firm administrative resolution with suspension or removal from office for violation of PBCFT regulations. This circumstance will be appreciated during the time that the sanction is prolonged.

TITLE III. ON INTERNAL TRAINING ON CAPITAL PREVENTION

Article 14.- Training

The obliged entity will adopt the appropriate measures so that its personnel have adequate knowledge of the requirements derived from the regulations on the prevention of money laundering and the financing of terrorism.

Specifically, employees will receive a training course at least once a year, and upon completion they will take a knowledge test. Staff attendance will be checked.

The obligated entity will approve the annual plan, proposed by the Compliance Officer, which must be based on the identified risks and will provide for specific training actions for managers, employees and agents, also including training actions in this regard.

The degree of compliance with the training plan must be documented annually.

Likewise, this Manual will always be available to all employees, and if it is modified or updated, you will be informed by email of said change or update.

TITLE IV. OF THE EXEMPTION OF LIABILITY

Article 15.- Exemption from Liability

The communication in good faith of the information derived from this Manual by employees to the Compliance Officer or, where appropriate, directly to the Prevention Body, will not constitute for them a violation of the restrictions on disclosure of information imposed by contract or by law. any legal or regulatory provision and will not imply any type of liability.

TITLE V. COMPUTER TOOLS

Article 16.- Computer Tools

Given the volume of the Client portfolio, for the identification of operations, the Company will rely on applications such as Excel and Access, using its databases, exploiting them with computer tools (Office).

Additionally, the Company will verify the names and identification document numbers of the Clients, as well as the amount of the transactions in order to avoid possible splitting of operations that should be communicated in the mandatory monthly communication.

In the event that the volume of the Client portfolio makes it necessary to use electronic means to extract operations, the Company will provide such means.

Likewise, computer tools will be configured so that centralized alerts are generated every time funds have been received from Clients:

a) For amounts greater than 10,000 euros.
b) Residents in countries, territories or jurisdictions included in Annex I of the Manual.
c) That they meet the status of PRP.

The recipient of these alerts will be the Compliance Officer, who must carry out a special examination of said operations.

To do this, the IT tools will have the following resources and measures:

- Client file: Each client has a personalized file within the computer system in which they can be consulted.

- All the client's personal data. Documents related to the
- client. Detail of the operations carried out with the
- Company.
- Mandatory fields: Tool intended to prevent the client or operation from being registered when all the client or operation data is not complete.

- Tax havens and non-cooperative territories: The computer system detects the presence (whether for reasons of nationality, residence, destination or origin of funds) of risk jurisdictions. In these cases, an alert will be activated that will warn of the need to adopt the planned measures.

- Persons subject to a ban on operating: The computer system detects the coincidence of the sender and beneficiary data with those contained in the OFAC, European Union and UN lists of persons or entities subject to a ban on operating and, as such case, it automatically blocks the execution of the operation.

- Activity: In the event that, when entering the professional or business activity in the Client File, any of those considered as risk activities are indicated, in accordance with the

Client Admission Policy or the Risk Operations Catalog, an alert will be activated that will warn of the need to collect additional documentation as the client has a risk profile.

Likewise, the computer tools will have the following features:

- Set up a blacklist of conflicting users.
- Notify of movements or transfers issued or ordered from countries or territories considered risky in real time.

- Detects provisions of funds made by third parties other than the account owner. Refund requests to accounts of third parties other than the account holder.
- Detects structuring, high-value transactions, inactive accounts, interconnected transactions carried out by different participants, coins enhanced with anonymity, operations related to opaque markets, mixer services, etc.).

- Detects Internet domain names through proxies or using domain name registrars (DNS) that suppress or redact domain name owners.
- Detects IP address associated with a darknet or other similar software that allows anonymous communication, including encrypted emails and VPNs.

TITLE VI. COLLABORATION WITH SEPBLAC OR OTHER AUTHORITIES

Article 17.- Collaboration with the Prevention Agency or other Authorities

The requirements that the Prevention Body or other Authorities may formulate to the Company will be attended to by the Compliance Officer, who will clearly prepare the responses to them within the period established by the aforementioned Authorities.

Once the deadline for sending the required documentation or information has elapsed without it having been provided or when it is provided incompletely due to omission of data that prevents the situation from being properly examined, the obligation established in this article will be deemed to have been breached.

In this sense, the Company will establish, within the framework of internal control measures, systems that allow it to respond completely and diligently to requests for information that the Prevention Body or other legally competent authorities on whether they maintain or have maintained over the previous ten years business relationships with certain natural or legal persons and on the nature of said relationships.

TITLE VII. REVIEW OF INTERNAL CONTROL PROCEDURES AND MEASURES

Article 18.- Review of Procedures

The Compliance Officer will be in charge of reviewing, on an annual basis, the effectiveness of the procedures and internal control measures aimed at preventing money laundering and the financing of terrorism, with a view to verifying adequate compliance with them. , recommending, where appropriate, the development of non-existing procedures, as well as the improvement or implementation of new controls for the detection of operations susceptible to money laundering.

Where appropriate, the effectiveness of the procedures may be evaluated by analysis of samples obtained from the operations carried out. Meettowritten record of the results of the review, the information communicated to the administrative body about said results and the proposed improvements.

All manuals, as well as the information, files or media related therein, will be accessible to clients who request it through the communication channels established for this purpose.