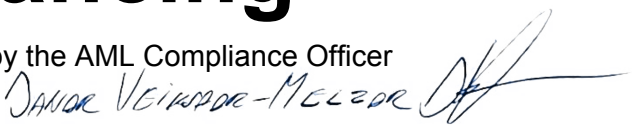
Ereus Policies and Procedures Manual for the Prevention of Money Laundering and Terrorist Financing

Compiled by the AML Compliance Officer
Signature: 

Policy approved by Audit and Risk Committee on 20 December 2021
Review date December 2022
This policy will be reviewed triennially by Audit and Risk Committee, unless there is a change in the Estonian legislative framework that requires it to be updated and reviewed sooner. Minor updates, for example name changes, will be made periodically on the authority of the Compliance Officer as required.

TABLE OF CONTENTS

CHAPTER

Annexes

Ereus Crypto Exchange

Policies and Procedures Manual for the Prevention of Money Laundering and Terrorist Financing.

1. CEO’S STATEMENT

The CEO of Ereus Europe OÜ (“Ereus”) considers Corporate Integrity, understood as the systematic commitment on the part of the company to uphold strict standards of ethical conduct,

to be a source to create stable value and essential for preserving society's confidence in the institution. Bearing this in mind, the policies that endorse the strict compliance with the legal framework governing the prevention of money laundering and terrorism financing become of great importance.
The CEO's commitment to this objective is set forth in the "**Manual for the Prevention of Money Laundering and Financing of Terrorism"** (here on the Manual) that defines the guiding policies for adequate prevention and control. It includes procedures for the detection and reporting of activities possibly linked to money laundering or the financing of terrorist activities. The appropriate application of this Manual requires that staff and senior management be familiar with its contents, related procedures, and norms that regulate these activities.
Compliance with the contents of this Manual is required for all Ereus employees.
Non-compliance with the criteria and guidelines contained in this Manual will lead to the corresponding responsibilities and sanctions.

2. SCOPE OF APPLICATION

The Manual will be applied to Ereus and will be binding for all employees and senior management. The contents of the Manual will prevail over other internal regulations that could come in conflict with these, excepting those that establish more strict conduct and/or prevention measures.

3. DEFINITION AND STAGES IN THE PROCESS OF MONEY LAUNDERING AND TERRORISM FINANCING

3.1 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 the above refer to the same process that we define as follows.
"The surreptitious introduction of illegally obtained funds into the legitimate channels of the formal economy" (United Nations).
"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" (International Monetary Fund).
Thus, money laundering is the process by which a natural or legal person, who is in possession of assets derived from unlawful activities, introduces them to the financial system to obscure the source of the illegally obtained monies, and making them appear to be legitimate.
Given the nature of the financial operations used for laundering money, it is possible that financial entities be used inadvertently as agents for investing funds coming from illicit or criminal activities, jeopardizing the stability, reliability and credibility of the institutions involved.

3.2 RISK MANAGEMENT

Risk Management refers to all activities whose purpose is to anticipate adverse events from occurring. This is achieved by designing and implementing strategies, processes and structures that minimize the impact of the losses.
Risk analysis is the study of events that affect company activities, and risk management is the application of strategies to avoid or reduce the costs of risk.

Hence, risk management and analysis include the following:

• Investigating and identifying the sources of risk
• Estimating the probability and evaluating its effects
• Designing strategies and procedures for controlling risk
• The optimum application of those strategies in the presence of uncertainty.

For this Manual, risk means the eventuality or possibility that Ereus could suffer damage, keeping in mind that the nature of its operations makes it particularly vulnerable to be used as an instrument to launder money and/or for the channeling of resources for terrorist financing, or as a means to conceal wealth generated from these activities.

The risk of money laundering and terrorist financing materializes in the form of COMPLIANCE or LEGAL risks, REPUTATIONAL risk, OPERATIONAL risk, and CONTAGION risk, all of which the entity is exposed to, having negative economic effects on its stability when it is utilized for such activities.

In this Manual:

Compliance Risk refers to the possibility of losses that Ereus could suffer if it is sanctioned or fined for any, or all damages, caused by failure to comply with the legal framework and/or contractual agreement.

Reputational Risk refers to the possibility of losses that the company could suffer, whether due to the loss of prestige, being portrayed poorly or being subject to adverse publicity in their role as a Virtual Asset Service Provider and its business practices, which could result in loss of customers, income or have legal implications for the company.

Operational Risk refers to the possibility of incurring in losses due to deficiencies, inadequacies, or failure in the systems, people or internal systems, or as a result of external factors.

Different types of operational risks that can be a source of substantial losses:

- Internal fraud: intentional misinformation of positions, robbery on the part of employees, the use of confidential information in favor of an employee account, etc.

- External fraud: refers to robbery, forgery, check fraud, damages caused by hacking IT systems, etc.

- Employee relations and workplace security:

Employee request for compensation, violation of labor laws regarding safety and hygiene, organization of labor activities, discrimination disputes, general responsibilities, etc.

- Practices with customers, products and businesses:

Abuse of confidence invested in them, misuse of confidential customer information, fraudulent use of bank accounts, money laundering, the sale of unauthorized products, etc.

- Damage caused to material assets:

Acts of terrorism, damage to property, arson, etc.

- Alterations in activity and system failures:

Hardware or software failure, problems with telecommunications, and failures in providing public services, etc.

-Execution, delivery and processing:

Errors entering data, failure in the administration of the collateral, incomplete legal documents, allowing unauthorized access to customer accounts, inadequate practices of counterparts different from customer, legal disputes with distributors, etc.

Contagion Risk refers to the possible loss that an entity can suffer, directly or indirectly, as a result of its practice or acting as a Crypto Exchange and being commercially tied to either a supplier, customer, correspondent bank, custody, or even a counterpart.

In order to implement a criterion which takes into account the minimization and management of risk, this entity determines the possibility of occurrence and impact based on:

- customer categories (high, medium and low risk customers)

- source of resources

- customer business activities

- geographic location where activity occurs - other elements

The factors that have been identified as high risk with regards to the above criteria are the following:

- Customers that appear in public watch lists as suspected of engaging in money laundering and/or terrorist financing

- PEPs

- Persons that act on behalf of their customers

- Civil associations and/or so-called non- profit organizations that are not under strict control or supervision

- Cash intensive businesses such as currency exchange houses and casinos

- Customers who due to the nature of the entity do not reveal the identity of the beneficial owner or major investor.

- Customers with criminal records and/or adverse credit history (issuing bad checks, closed accounts, embargoes, etc.)

- Customers that handle large volumes

- Countries identified as promoting and financing terrorism

Risk Management Process

- Identify: at the institutional level, lines of business, products, transactions

- Measure: risk for each customer, product or service, by geographical factors, and by legal and regulatory risk.

- Monitor: implementation of "Know your Customer and Employee” Policy

- Control: discontinue an activity, product or line, using mitigation techniques, and contain and monitor risk.

It is inevitable that not only an initial check be conducted when the account is opened, but also it needs to be followed by an additional personalized monitoring of each one.

In order to identify the risks that exist in the different activities and customer categories, our Compliance Department is in charge of implementing adequate control measures.

There is continuous monitoring of customer activity in order to anticipate trends and to be able to detect any unusual activity. In this way any unexpected or suspicious operation that could indicate risk will be reported immediately to the Compliance Officer.

The following tasks are performed:

- Identify inherent risks in the different lines of activities and customer categories.
- Evaluate the possibility of them occurring and the possible impact.

- Implement control measures that are suitable for mitigating the different types and levels of risk identified.

- Monitor permanently the results of the controls that are in place and their level of effectiveness in order to detect unusual or suspicious transactions (STR) and to correct deficiencies that exist in the risk management process.

Risk Matrix

Ereus Risk Matrix is used to identify areas where there is a higher risk of money laundering and terrorist financing, and also to determine the Company's Risk Profile.

Risk is estimated based on the person, however in order to apply that risk to the whole account, it is necessary to consider the type of account (investment, for transactions, or both). That is, the risk assessment is performed based both on the person (based on four characteristics) and the type of account being opened in order to consider the customer as a whole.

Methodology for Evaluating Risk

Once the risks have been identified, it is necessary to evaluate them taking into account not only the probability that the risks occur, but also the consequences that these would have with regards to losses or damage caused.

PROBABILITY X IMPACT = RISK LEVEL/RATING

Probability

Three levels of the probability of risk occurring can be identified:

RATING	**DESCRIPTION**
VERY PROBABLE	Huge consequences, damages or effects
PROBABLE	Moderate level of impact
IMPROBABLE	Small consequences or effects

Impact

Rating	Risk Level
1	LOW
2	MEDIUM
3	HIGH
4	VERY HIGH
5	EXTREME

The use of the following risk matrix allows us to combine probability with impact in order to obtain a risk rating range:

RATING	DESCRIPTION	DECISION
5	Extreme	It is highly likely that something will occur and /or that it will have very direct consequences. Do not authorize transaction.
4	Very High Risk	Do not authorize transaction.
3	High Risk	Risk likely to happen. Do not authorize transaction until risk is reduced.
2	Medium	Possibility of risk occurring and/or moderate Consequences.
1	Improbable	Improbable that something will occur. Complete the transaction.

The appetite for risk refers to the amount of risk that the entity is willing to accept in order to achieve its objectives and serves as a guideline for the risk management strategy. Bearing this in mind, the entity must determine which risks they are willing to accept under normal due diligence procedures, which risks are unacceptable, and which risks will be considered on a case-by-case basis, and will only be approved if enhanced due diligence procedures are applied.

Limits on transactions for high risk products can be established, senior staff authorization can be required for the approval of certain customers, or customers can be categorized based on different means of identification and verification.

A customer can go from being low risk to high risk if they change the way they operate, or demand new services. On the other hand, a high-risk customer can be classified as low risk if the firm considers that its business relationship over time has been satisfactory.

An example of a worksheet that takes into consideration different types of customers, within this risk category, the probability, impact and rating, as well as the risk treatment that the entity could consider:

RISK CATEGORIES: CUSTOMERS

TYPE	PROBABILITY	IMPACT	RATING	TREATMENT
New Customer	Probable	Moderate	2	Standard verification and control procedures
Customers with high flow of operations	Probable	Large	3	Purpose of the account and client background, volume and the frequency of the transactions
Unregistered Charitable Organizations	Very probable	Large	4	Refusal
PEPs	Probable	Large	5	Senior staff authorizations

Keeping records and conducting evaluations on a regular basis are essential for maintaining an effective prevention program.

The money-laundering prevention program cannot be a static tool since risk can evolve with time (changes can occur in the customer base, products, services as well as in the legislation). For this reason, it is necessary to develop ways of verifying, on a regular basis, if the money laundering prevention program is working effectively, and if it’s not, then make the necessary changes.

Operations Report

It is the responsibility of the Compliance Department to confirm not only that the Crypto Exchange’s customer portfolio complies with the first stage (customer identification and control of customer information), but also that the resulting profile created based on the data submitted is correct and in accordance with the transactions conducted by the customer.

In order to do so, the Compliance Department implements the following measures, all of which are different types of control that allow the Department to verify that the profile initially defined remains the same, and to confirm that the customer profile that is defined is correct.

Control Measures. Transaction Monitoring Systems

The transaction monitoring system includes the following controls that are conducted annually and/or every six months.

Comparison between the Declared Potential and the Real Potential

When initiating a business relationship with a customer, the account manager must obtain data to measure the potential of the customer in order to be able to classify them or to determine their profile.

To verify the data, the information collected initially is compared with the customer's actual operations.

If deviations occur, the Compliance Department will work with the account manager to modify the profile accordingly.

This control is conducted every quarter.

Comparison between the number of deposits estimated and the number of deposits actually completed.

When the profile is complete, the account manager has an idea of the average number of transactions that the customer might carry out. This report consists of comparing what was initially anticipated with the number of transactions that were actually carried out.

This control is carried out every quarter.

Analysis of Movements Considered Material / DEP/RET Report

This control consists of an analysis of the consistency existing between the movements considered material (exceeding EUR 100,000) and the account and customer profile these are tied to.

A monthly report that tracks material movements by the customer, their profile, and their potential will be issued If:

Customers in absence	Probable	Large	3	Determine identify. Verify provided documents

the customer's profile is not consistent with its operations, then further analysis of the case is carried out together with the account manager.

How are controls conducted and monitored?

Report/Monitoring Alert

Account managers review reports/alerts and send an automatic responses to PLD Analyst

Analyst studies response when the controls are in place, certain alerts are triggered off when an account acts outside of its profile or operates outside the limit anticipated.
When this occurs, the Compliance Department sends a report to the Account Manager with the monitoring alerts requesting an appropriate explanation.
The Account Manager receives the message electronically.
The message must be returned to the Analyst with comments.
If the latter considers that the comments are not sufficient, then the Account Manager shall review the case further and if necessary provide additional supporting documentation.
If there is no plausible explanation for the activity, or there is some doubt as to the legitimacy of the source of the funds, then the Compliance Officer must be notified.

The Compliance Officer will be responsible for adopting the appropriate measures and will report, if necessary, these activities to the authorities of the Estonian Financial Intelligence Unit ("EFIU").

In addition, information about natural or legal persons who carry out transactions involving money in local or foreign currency, or securities that are easily convertible, in amounts exceeding EUR 10,000 as well as transactions that involve a single person exceeding this amount during the same month, must be reported to the Estonian Financial Intelligence Unit ("EFIU").

INDEPENDENT REVIEW OF THE COMPREHENSIVE PREVENTION SYSTEM

An independent review of the Comprehensive Prevention System must be conducted annually.
External Auditors will be in charge of the review.
The review will follow the format established by the Estonian Financial Intelligence Unit ("EFIU") and it will include an evaluation of the policies and procedures of this Manual.

The review will include an opinion as to the adequacy and implementation of the policies and procedures adopted by the institution to prevent the institution from being used for laundering funds coming from criminal activities or for terrorist financing. The review must point out the deficiencies or omissions that are considered important, and it must make recommendations for resolving these issues and adopting corrective measures.

3.3 DEFINITION OF TERRORIST FINANCING

The United Nations has defined terrorist financing as the following:

“A person by any means, directly or indirectly, unlawfully and willfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out:
(a) An act which constitutes an offense 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.”

Estonian law takes into account this definition and defines terrorist acts as the following:

“Terrorist acts are crimes that are committed with the purpose of causing death or serious bodily injuries to a civilian or any other person that does not participate directly in hostilities of an armed conflict, when the purpose of this act, that is revealed by the nature of the act, or its context, is to intimidate a population or to force a government or international organization to act or to abstain from doing so.”

According to another definition, the main objective of terrorism is to “intimidate the population or to force a government or an international organization to act or, to abstain from doing so." Unlike the main purpose behind other kinds of criminal activity which is gaining wealth.
Even though there are differences between the final objectives, terrorist organizations require financial support to achieve their activities. A successful terrorist organization, like any other criminal organization, is one that can set up and maintain an effective financial infrastructure. In order to do so, they must develop sources of financing, a way to launder money and ensure that these funds are available to be used to purchase the materials and logistic elements necessary to carry out terrorist acts.

Experts, in general, consider that terrorist financing comes from the following main sources:

The first is financial support that comes from States or Organizations, and the other is profit obtained from wealth generating activities.

Similar to the wealth of criminal organizations, terrorist funding can be derived from criminal or other illicit activities, from legitimate sources or a combination of both legal and illegal sources.

The latter is a key difference between the modus operandi of terrorist groups and other criminal organizations. Community donations and fundraising are very effective ways of terrorist financing.

Frequently, funds are obtained in the name of charitable or benefit organizations.

Even though it might seem strange that money from legitimate sources needs to be laundered, terrorist groups often need to conceal or disguise their ties with legitimate funding sources.

Thus, they need to find ways to launder these funds without calling the attention of authorities.

Terrorists and their supporting organizations, often use the same money laundering methods used by criminal groups. Another important aspect of terrorist financing that makes it difficult to detect is the size and nature of the operations involved. Terrorist acts do not always require large amounts of money, and the operations used to obtain the money usually are not very complex.

3.4 STAGES IN THE PROCESS OF MONEY LAUNDERING

Money laundering is carried out through an array of different activities. In this sense, we can say that money laundering is not just one single operation, but rather a sequence of transactions that can be grouped in three distinct stages:

A) Placement, Incorporation, Accumulation

This consists of the placement of illegally obtained monies, mainly large amounts of cash, into the formal economy, especially the financial sector, and by defeating all the established monitoring measures transforming this money into negotiable financial instruments.
For criminals, this is usually the riskiest stage in the process of money laundering.

Financial institutions play an instrumental role in the detection of such activities and by keeping tight monitoring and screening methods they can avoid becoming part of the process.
The methods used to place funds – mainly cash - obtained from illegal activities into the financial system are varied and there are several combinations possible. In our case, our concerns are Investment transactions.

It is common to incorporate cash into the financial system by making a series of smaller deposits (structuring, also known as “smurfing”) in order to overcome the registry and screening procedures that are generally in place to detect such transactions. (See below).

B) Layering, Concealment, Dispersion of Transactions

Once the funds have been placed into the financial system, it becomes more difficult for law enforcement to trace these monies back to the illegal activities that originated them, whether drug trafficking or others.
The main purpose of this second stage is to distance these proceeds from the criminal activities that originated them, concealing the source as well as the true ownership of such funds.

This is achieved though several complex financial transactions such as international wire transfers.
By layering a series of transactions, these criminal proceeds generate a number of financial instruments and documentation, which makes it extremely difficult to trace back the origin and the true ownership of the funds.

C) Integration, Investment or Recycling.

During this last stage, after having gone through the stages previously mentioned, the illicit funds go back to the criminal groups from what seem to be legitimate sources, such as transfers between companies, returns from investments and other legitimate activities.

There are three main objectives to the laundering process:

1. To create an intricate trail of paperwork and documentation
2. To disguise the origins and true ownership of the funds.
3. To commingle ill-gotten monies with legitimate transactions.

Although money laundering tries to make these funds appear legitimate, this process will never achieve its aims. The proceeds from criminal activities will never be legitimate money.

Since our country is a financial market known worldwide for its full freedom of capital movement and protection of customers' identity, we must be extremely wary so as to prevent these market advantages from being used for illegal activities.

As the aforementioned shows, financial institutions are the means by which the transactions involved in the different stages of the money laundering process are carried out. Therefore, by being able to detect and identify these activities, the financial institutions play an instrumental role in the prevention of criminal activities and they protect at the same time their reputation and that of their customers and employees.

4. REGULATORY FRAMEWORK

4.1 INTERNATIONAL REGULATIONS

Main International Organizations and Regulations:

- The United Nations was the first international organization to start substantial work to combat money laundering worldwide.
- The Financial Actions Task Force (FATF). It is the main international body established to combat money laundering and terrorist financing. It has issued the "Forty Recommendations" report and the "Nine Special Recommendations on Terrorist Financing" report.
The international community considers these to be the universal standards.

- The Basel Committee. It develops standards, guidelines and best practices for a wide range of banking supervisory matters. It has issued three documents on to the prevention against money laundering:

1) “Prevention of Criminal Use of the Banking System for the Purpose of Money Laundering" (1988);
2) “Customer Due Diligence” (2001);
3) “Know your Customer Risk Management” (2003).

- Wolfsberg Group Principles:

1) Statement Against Corruption (2007);
2) Risk Based Approach for Managing Money Laundering Risks (March 2006);
3) Statement on Monitoring Screening Transactions (September 2003);
4) Anti-Money Laundering Principles for Correspondent Banking (November 2002);
5) Statement on the Financing of Terrorism (January 2002);
6) Anti-Money Laundering Principles for Private Banking (Revised version May 2001).

4.2 DOMESTIC REGULATIONS AND LEGISLATION

Laws:

Money Laundering and Terrorist Financing Prevention Act1
Passed 26.10.2017
RT I, 17.11.2017, 2
Entry into force 27.11.2017

Source: https://www.riigiteataja.ee/en/eli/509012020001/consolide

Set forth below there is a brief summary of the latest changes in the laws and regulations previously mentioned.

In order to comply with the new regulations, the following becomes compulsory for crypto businesses:

- Revision of the internal AML procedures:
- Appointment of a Compliance Officer:
- Assessment of the experience and business reputation of the management:

- The management must determine whether new business relations are established with persons from outside the European Economic Area or with e-residents;

- Compulsory identification and verification of data with the help of information technology means (specific regulation applies) where a business relationship is established with an e-resident or a person from a country outside the European Economic Area or whose place of residence or seat is in such country (unless it is possible to carry out identification face-to-face);

- The Compliance Officer must possess the competence, means and access to relevant information across all the structural units of the business;

- The so-called fit & proper test. The Financial Intelligence Unit will require documentation on management's level of education (at least secondary education), work experience, character and responsibilities of earlier posts, extra training etc. The education, knowledge, experience and skills will be evaluated against the responsibilities and area of activity of the manager in order to assess their capability to understand the risks and carry the responsibility deriving from it. The correct business reputation is presumed until proved otherwise. This is evaluated based on earlier activities such as media coverage, punishments, court dealings, participation in management of companies etc.

Reputation is seen as of a more permanent nature than the current checks of the criminal record and therefore it is not subject to legal expiration nuances. The prerequisite for an impeccable reputation is the absence of any circumstance precluding high reputation.

The registered office of the company, the seat of the management board and the place of business must be in Estonia or a foreign company operating in Estonia through a branch which is registered in the commercial register and has its registered office and head office in Estonia:

- The registered office of the company as seen on the commercial registry is in Estonia;
- The seat of the management board is in Estonia meaning that essential functions of the management and control of money laundering are carried out, including the continuity of functions necessary for the conduct of the business;
- The place of business is the factual location of the business and must include the location of the Compliance Officer.This does not necessarily have to match the registered office address.
- Existence of a payment account with a credit institution, an electronic money institution, or a payment institution established in Estonia or a Contracting State of the European Economic Area providing cross-border services in Estonia or having established a branch in Estonia.
- Share capital of at least EUR 12,000.

The Financial Intelligence Unit will have a legal right to revoke the existing license in case it identifies non-compliance, e.g. that the crypto business does not carry out its activities in Estonia or that its management board is not located in Estonia.

5. CUSTOMERS

5.1 DEFINITION OF CUSTOMER

Although the regulatory bodies have not issued an official definition, by “customer” we understand the following: any person, natural or legal entity, with whom Ereus has a business relationship by providing a service or product, offered under the scope of activities proper to their field of expertise and in compliance with the established legal and regulatory framework. In addition, in those cases in which customers are operating on behalf of third parties, the latter (known as “Customers of Customer”) shall be considered as customers.

5.2 WHOLESALE AND RETAIL CUSTOMERS

Following domestic regulations, Ereus distinguishes among “Wholesale” Customers and “Retail” Customers within the framework of Customer Identification and Know Your Customer policies. There are fewer identification requirements for Retail than for Wholesale Customers, In addition, Retail Customers are not subject to “Know Your Customer” policies.

Categorizing customers in these two groups allows for a more effective money laundering risk management, maximizing at the same time Ereus business management.

A customer is considered as a “Retail” customer when the total amount of their transactions, including custody transfer, over the course of one calendar year remains within EUR 30,000 threshold (thirty thousand Euros), or equivalent in other currencies.

5.3 CUSTOMER ACCEPTANCE POLICY

Customer acceptance will be based on the following guidelines:

- Those who can’t be properly identified will **NOT** be accepted (See Customer Identification 7.3)
- Customers who have been blacklisted as “Unwanted Customers” by Ereus will **NOT** be accepted.
- Customers listed under OFAC SDN watch list and/or United Nation’s “Consolidated List” will **NOT** be accepted.
- Ereus will **NOT** establish business relationships with “anonymous customers” or those who use fictitious names.
- Those who hold businesses that due to the nature of the business make it impossible to verify its legitimacy or that of the funds being inconsistent with their financial status will **NOT** be accepted.
- It is a requirement of Ereus that customers submit the relevant documentation in

due course and proper form, and those who fail to comply will **NOT** be accepted as customers.
- Those people who are suspects, based on reliable information, of being involved in any sort of criminal activities, mainly related to drug trafficking, terrorism and organized crime will **NOT** be accepted.

5.4 DEFINING THE PROFILE OF THE CUSTOMER

The officer in charge of the business relationship will establish the Profile of the customer, based on the supporting information and documentation found in the customer's dossier or file.

The Operating Profile is defined based on the maximum total amount, both cash and securities custody, to be transacted over the course of one year.

The operating limits in place must be revised once a year or if there are significant changes in the nature and volume of the transactions conducted by the customer.

6. CUSTOMER RISK CATEGORIZATION POLICIES

In order to know the level of due diligence applied to the customer in the processes of acceptance, identification, and Know Your Customer, those who are considered as Wholesale Customer will be categorized under a risk-based approach for the prevention of money laundering and terrorist financing.

The Risk Factors considered and the Methodologies used in the categorization approach are listed below.

6.1 RISK FACTORS

Ereus has considered the following risk factors:

a) Geographic location
b) Activity
c) Politically Exposed Persons (PEPs)
d) Materiality
e) Customers of Customer

6.1.1 Geographic Location

There are certain geographic locations considered as a higher risk for money laundering and terrorist financing.
The Estonian Financial Supervision Authority ("EFSA") has listed the following as higher-risk countries:

1) Those that are not members of the Financial Action Task Force (FATF), or regional FATF-like bodies groups of similar nature such as the Financial Actions Task Force of South America

(GAFISUD), Caribbean Financial Action Task Force (CFATF), Middle East/North Africa Financial Action Task Force (MENAFATF), Asia/Pacific Group on Money Laundering (APG), and so on.

2) Those countries being subjected to sanctions by the aforementioned groups for not being compliant, or not being sufficiently compliant with FATF recommendations. (See Annex 1 –High-Risk Geographic Locations- for list of countries currently listed under those conditions).

Customers considered as high risk due to their geographic location are those who have substantial connections in a high-risk country/city, that is:

- Companies/Customers that hold property, residence, offices or headquarters in a high-risk country.
- Companies/Customers whose majority shareholders or beneficiary owners are located in such countries.
- If there are any other substantial connections/links that might be identified.

Although Nationality is an important element it is not determining to classify someone as a high-risk customer.

6.1.2 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.

Activities considered high-risk include:

• Casinos, Gaming Centers, Racetracks
• Money Remittance Companies
• Non-Governmental Organizations (NGOs)
• Financial Investment Corporation
• Arms, weapon manufacturers, distributors and dealers
• Precious metals distributors and dealers
• Antique dealers
• Professionals who act as intermediaries (Lawyers or accountants that manage their customer's funds in their accounts)
• Cash-intensive businesses (such as supermarkets, restaurants/bars, duty-free shops, parking garages, etc.)

High-Risk Customers are those who possess **significant connections** to activities considered high-risk. The account official will have to determine whether the connection is significant or not. There is a significant connection if the company is involved in or if a large portion of the company's turnover comes from high-risk activities.

6.1.3 Politically Exposed Person (PEPs)

Public corruption is considered as 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 with them, family members or close associates, might pose a legal or reputational risk to our Entity.
Politically Exposed Persons (PEPs) are those who have a high political profile, who hold or have held public office, whether in their country or abroad, such as heads of state or government, politicians, high ranking government officials, senior judicial officials, a high-ranking officer in an armed force, political party leaders, members of the board or senior executives of state-owned companies and entities.

Having business relationships with PEPs family members:

1) close associates.
2) or companies controlled whether directly or indirectly.
3) by PEPs represent risks to the reputation of the company similar to those damages caused to the reputation of PEPs themselves.

These three groups are defined as follows:

1) Spouse; Parents or the spouse or partner of a parent; Child or the spouse or partner of a child; Siblings.
2) Any person who is publicly known to have close business relations with the PEPs.
3) Companies in which the PEP is the majority shareholder (holding over 50% of the assets/equity) or final beneficiary (holding corporate will).

If corrupted PEPs were to use the services of our company, it would cause irreparable damage to our reputation and therefore lead to distrust of the general public. This is why we must have access to information about the new customer and evaluate all the public information there is available in order to decide whether or not the new customer falls under the PEP category.

It is not realistic to think that we will be able to investigate every family member, business or political associate of the potential customer. We will decide the need to go more in-depth with the investigations depending on the potential customer’s volume of transactions, behavior patterns, background, reputation of their country of origin, how reasonable their explanations are, etc.

We should remember, however, that it is very unlikely that PEPs (or their family members or friends) will come forward and introduced themselves as such. It is possible that many will try to disguise their status.

Ereus will use the databases provided by specialized agencies containing the profiles of PEPs (herein after PEPs list) as a tool to support their activities throughout this process.

6.1.4 Materiality

The materiality of the relationship with a customer represents a risk factor. In order to evaluate it, we will use the assets under management (AUM) value stated in the customer's profile as reference.

6.1.5 Customers of Customer

Those persons (natural or legal entities) that conduct operations through a direct customer of Ereus, are considered indirect customers and called "**customers of customer".**

In such cases the business relationship is established between Ereus and the direct customer, but the transactions that the latter conducts in our institution are actually done on behalf of a third party.

This is our direct customer's customer. In such cases Ereus doesn't have a direct relationship with the third party, and this is why enhanced due diligence processes are required.

In addition, they shall be able to identify the beneficiary owners of the transactions when so required by due diligence processes.

For identification purposes, a statement describing the type operations each customer conducts shall be included in the customer's registry form, in order to establish whether they are operating in their own interests or on behalf of third parties.

A list of all the people involved will be requested in order to complete these transactions.
It should state: first name, last name, I.D. number, type of document and amount transacted.

All of which must be cleared by the Compliance Officer.

With regards to our institution, we will by all reasonable means try to identify the beneficiary owners of the funds as well as the true motives (financial, legal, etc.) as to why this type of intermediary operating process has been chosen.

For record-keeping purposes and to know our Indirect Customer (Customers of Customer) we will request information that will allow us not only to identify and validate the identities of the Customer and that of the Beneficiary owner of such funds (partners, associates or majority shareholders for legal persons), but also to monitor their financial, business activity and the source of the funds channeled through Ereus.

If the customer refuses to provide information about the beneficiary owners of any one of the transactions, the controlling body will evaluate and assess whether or not this is an unusual or suspicious transaction that should be reported to the Financial Analysis and Information Unit.

6.2 RISK CATEGORIES

Ereus categorizes customers under three risk levels (low, medium and high) depending on the information collected at the opening of the account. Ereus categorizes the risk factors taken into account and classifies them according to the following matrix.

Risk Category Matrix for Wholesale Customers

* Transactional Profile (Annual), if not applicable, Total Volume Transacted in USD (calendar year) Customer Risk level shall be used to determine:

• Level of AML compliance of such relationship
• Level of Due Diligence.

The form shown in Annex 2 will be used to categorize customers' risk levels, according to the parameters aforementioned.

For those customers who do not fall under any of the risk categories mentioned in sections 6.1 and onwards, risk will be determined based on the total annual amounts invested.

Those customers whose annual investment is within the EUR 250,000 threshold will be categorized as low-risk.

Those who Company name transact EUR 250,000 to EUR 500,000 annually will be considered medium-risk and finally, those who operate over EUR 500,000 will be considered high-risk.

When customers do fall under any of the risk factors aforementioned, the total annual investment will also be used as a variable to determine risk levels. Up to EUR 100,000 will be low-risk, from EUR 100,000 to 250,000 will be medium-risk and over EUR 250,000 will be high-risk. The variable Total annual investment will not be necessary when dealing with PEPs, since they are always considered as high-risk customers.

6.2.1 Officer in Charge

a) Task/Process Officer in Charge
b) Keeping list of countries considered "Risky" updated (every six months)
c) Compliance Officer Reviewing factors and methodologies for Risk
d) Classification (Annually): Customer Classification by Compliance Officer

6.3 CUSTOMER ACCEPTANCE

Customer Acceptance level will depend on the risk rating assigned to that customer.

Risk Category Authority:

- Low: Account officer
- Medium: Compliance Officer
- High: Compliance Officer

In order to speed up the process, acceptance notifications can be done via e-mail.

7. KNOW YOUR CUSTOMER POLICY

7.1 OBJECTIVES

Assets Under Management (AUMs)*	Customers with no risk factors	Customers under Geographic Location and Activity risk factors	PEPs
Over EUR 500,000	High	High	High
EUR 250,000 - 500,000	Medium	High	High
EUR 100,000 - 250,000	Low	Medium	High
EUR 30,000 - 100,000	Low	Low	High

Knowing our customers is an essential element in our line of work.

By obtaining information on the source of the funds transacted by customers, Ereus can protect itself from being used to conceal illegally-obtained funds.

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

KYC Due Diligence (in terms of requirements, acceptance level and how frequently information is reviewed) is connected to Customer Risk ratings.

7.2 DUE DILIGENCE

The documentation that each customer will be requested depends on the risk category they were assigned when the account was opened.

Those customers Ereus considers as low-risk will be requested to fill out a registration form with their personal and contact information. If there is any change in the information, such as

address or telephone number, the customer must inform the company and replace the old registration form by a new one with the updated information.
A copy of the customer's I.D./Passport must be enclosed.

The company must check against the PEP lists available to make sure the new customer doesn't fall under that category.

Customers considered medium-risk, are requested to provide the same information as the low-risk customers, plus supporting documentation, such as a utility bill, as proof of address. They are also required to fill out a "Know Your Customer" form, in which they have to state the source of the funds, estimated annual income, estimated net assets or equity, and estimated total annual investment.

Customers considered high-risk, are subject to enhanced due diligence. This means that they not only will be requested to follow the general procedure, but also a detailed report of the circumstances must be filed (see annexes) explaining all the variables that were considered to create such profile. The report must be supported by pertinent documentation, any source of information that states and explains the customer's assets and financial position and/or the source of the funds.

The business relationship must be approved by the Compliance Officer. Additional information must be collected for certain Customers, Products or Services categories.

Customers who fall under the PEPs category must always comply with these requirements since they are considered high-risk regardless of the total amounts transacted.

Evidence required based on risk level

Low Risk	Medium Risk	High Risk
• Identification* • Lists • Supporting Documentation**	• Manual Validation	• Internet • Report • Supporting Documentation***

* for example: copy of I.D. card
** for example: utility bill
*** for example: latest Tax Return

7.3 CUSTOMER IDENTIFICATION

The main purpose of Customer Identification is making sure you know, within reason, the true identity of the customer.

All customers must be identified by any of the following identity documents:

- Passport
- I.D. card
- Drivers License

All of the above must be picture IDs. Expired or deteriorated identity documents will not be accepted.

7.3.1 Registration Form

The following information must be comprised for the Retail Customer:

1) Natural Person
- Full name and last name
- Identity document
- Address and phone/fax number/email

2) Legal Person
- Name and Type
- Address and phone number
- Tax Identification Number (RUC), if applicable
- Identification of the natural person who performs the transactions on behalf of the legal person following the aforementioned procedures, and documentation that proves the legal capacity of the representative.
- Identification of beneficial owner.

7.3.2 File

The following information must be comprised for the Wholesale Customer:

1) Natural Person:

- Full name and last name
- Place and Date of Birth
- Type and Identity Card number and issuing country
- Address
- Telephone/Fax number/e-mail

- Marital Status (if married, spouse's name and identity card number)
- Profession, trade or main activity
- Income
- Statement whether they represent themselves or act on behalf of a third party.
- Personal/bank references.
- Know Your Customer form, stating the source of the funds, estimated annual income, estimated net assets and estimated total annual investment.

In addition, a copy of the customer's identity document must be kept in the file.

This information must also be collected for all accountholders, representatives and all persons authorized to act on the Customer's (Natural Person) behalf.

The natural person's annual income information will be requested only if this income is a source of the funds transacted by the customer.

2) Legal Person:

- Corporate name/DBA
- Type of business entity
- Date of incorporation
- Country of incorporation
- Legal address
- Telephone/fax number/email
- Tax Identification Number (RUC), if applicable
- Main business activity
- Volume
- Turnover
- Identity of the natural person who performs the transactions on behalf of the legal person and documentation that proves the legal capacity of the representative
- Supporting documentation: certified copy of the articles of incorporation or bylaws, copy of
- taxpayer registry, documentation that certifies the legal capacity of the representative, agent, etc.
- Affidavit of beneficial owner and copy of his/her I.D.
- Personal/bank references
- Know Your Customer form stating the source of the funds, estimated annual income, estimated net assets/equity and estimated total annual investment.
- Last two balance sheets
- Minutes of general assembly meeting and the board of directors, titles and responsibilities.

- The information in section 1) above will also be requested for natural persons who act as administrators, representatives, agents and any other person authorized to act on behalf of the customer legal person.

The natural person's annual income information will be requested only if this income is a source of the funds transacted by the customer. All partners must be identified when dealing with Limited Liability Companies. The majority shareholders – those with a 10% share or more – must be identified when dealing with Corporations. If the partners or shareholders are legal persons with a 10% or above share, the owners of such legal entities must be identified and therefore obtain the identity of the natural persons behind the legal entities.

When the customer (or owner or majority shareholder) is a public company, listed in a stock market, subject to regulatory disclosure requirements, it is not necessary to seek to identify or validate the identity of the shareholders.

When dealing with trusts one must understand the substance and form of the legal entity. The identities of the settlor, trustee or person exercising effective control over the trust and beneficiaries must be verified.

See Annex 3, Customer file, for identity information requirements (natural and legal persons).

7.3.3 Updating Information

- Customer's information and/or documentation must be updated annually or under one of the following circumstances:
- Ereus modifies its customer identification regulations
- If customer information is insufficient or out of date
- At the request of the compliance officer within the framework of an ongoing investigation
- At the request of the auditors
- If any Red Flags are detected
- If there are any significant changes in the customer's behavior patterns

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

7.4 VERIFICATION AGAINST WATCHLISTS

7.4.1 Scope

- OFAC List: List issued by the Office of Foreign Assets Control (OFAC), USA - http://www.treasury.gov/offices/enforcement/ofac/sdn/
- UN List: List issued by The United Nations
- List of "Unwanted Customers"

The Compliance Officer at **Ereus** will put together a list of natural and legal persons who are not wanted as customers, which shall include as follows:

- Those people/companies that have appeared in publications as having ties with the organized crime, money laundering and terrorist financing.
- Customers that have been subject to a STR (Suspicious Transaction Report) and therefore the Committee for the Prevention of Money Laundering and Terrorist Financing ("The Committee") decided to include in this list.
- Those people, natural or legal entities, the committee has decided not to accept.
- PEPs List. List issued by companies providing PEPs identification services and managed by the Compliance Officer.

All customers, including shareholders (if dealing with closely held stock corporations, and representatives if there were any), beneficiaries, suppliers and counterparts will be checked against the OFAC SDN list, the "Unwanted Customers" list and the PEPs list.

7.4.2 Opportunity

All persons, natural or legal entities, must be checked against the watch lists before being accepted as customers.

The Wholesale Customers database will be checked against PEPs lists at least every six months.

If any potential customer/supplier/employee/beneficiary is found in the OFAC and "Unwanted Customers" list all ties of that potential customer with the Entity will be terminated, and an "Unusual Transaction Report" will be issued.

In case any potential customer is included in the PEPs list, the Compliance Officer approval will be necessary.

7.5 FINANCIAL AFFIDAVIT

All Wholesale Customers and those customers the Compliance Officer considers will be required to provide a Financial Affidavit (which will be included in the customer's file).

Special situations

If the funds originated from one specific event (like the sale of real estate), the customer will be allowed to present supporting documentation that verifies the source of such funds.

Event declared by the customer	Documentation required

Sale of Real Estate	Copy of public deed of sale or Promise to purchase and sale, where amount is stated
Sale of a Vehicle	Copy of deed of sale, certified by public notary
Compensation / Severance Payments (Insurance/Job)	Copy of certificate of payment issued by insurer or employer
Pension/retirement	Copy of settlement
Gambling	Copy of certificate issued by the gambling company certifying that the customer has won and the specific amount
Bonds	Copy of settlement

7.6 KNOW YOUR CUSTOMER FORM

7.6.1 Scope

The “Know Your Customer” form must be filled out by the High and Medium Risk customers as well as those customers the Compliance Officer considers must do so.
This will be done following the Best Practices procedures in the industry.

The “Know Your Customer” form must include:

- Reasons why the customer wants to establish a relationship with the Entity.
- Financial situation and business activity, in order to be able to clearly identify the source of the funds to be transacted with.
- Checking consistency between the expected activity (Transactional Profile) with the assets and financial position.
- Affidavit stating legality and origin of the funds.

The Know Your Customer form must be filled out and sent to the Compliance Officer. (See Annex 4)

7.6.2 Supporting Documentation

High-risk customers as well as those customers the Compliance Officer considers must do so, have to submit supporting documentation to verify their assets and financial position and (if necessary) their transactional profile. Some examples of this documentation are as follows:

Natural Persons:
• Pay Slip
• Tax return

Legal Persons:
• Balance sheet of its last fiscal year

• Tax return

7.6.3 Customer Dossier
All Customers will have a dossier, that will include the information and documentation required according to the level of due diligence applied.

7.6.4 Opportunity
Know Your Customer form will be filled out when:
• When conducting client risk categorization procedures
• When there is a Red Flag
• At the request of the Compliance Officer

7.6.5 Updating Information
During the time the Customer has business relationship with the Company, it is normal and foreseeable that they will change some of their personal and financial characteristics. If we compare the customer's current transactions against information that hasn't been updated, we might be misled into thinking there's suspicious activity when in fact there isn't, or vice versa. The information must be updated annually and/or if any of the situations covered in 7.3.3 happen.

7.6.6 Follow-Up of the Relationship with the Customer
The type of transaction the customer conducts or requests as well as the amounts involved in such transactions should always be controlled to make sure they are consistent with the customer's business activity, if the documentation available does not validate such transactions then appropriate records must be obtained in order to do so.
"Know Your Customer" should be enforced throughout the relationship with the customer, not just at the beginning of it. The factors to monitor are: types of transactions conducted, amounts involved and how these are carried out.
The "Know Your Customer" Policy must be in place for the full length of the customer's business relationship with The Company.

8. MONITORING POLICY AND SUSPICIOUS TRANSACTIONS REPORT
Transactions must be monitored in order to detect suspicious activities.

8.1 DEFINITION OF SUSPICIOUS TRANSACTION
Our legislation defines a **Suspicious Transaction** as:
"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 origin."
The Inter-American Drug Abuse Control Commission (CICAD) of the Organization of American States (OAS), defines **Suspicious Transaction** as those transactions, completed or not, complex, unusual, significant, any kind of non-habitual transaction and all transactions that

although are not significant are recurrent in time, that appear to serve no evident financial, business or legal purpose.

8.1.2 Red Flags for Centralized Monitoring

The following numerical parameters have been set up in order to follow up the activities of established customers at product level:

1) Amount of annual transaction by type of operation vs. limit established.
An anomalous transactional behavior represents a Money Laundering risk factor.

An anomalous behavior is:
a) A deviation in the customer's behavior compared to what had been anticipated, whether regarding the amounts, volumes, or types of products.
b) A deviation in the behavior compared to its standard behavior.
All Red Flags must be analyzed by the Compliance Officer following the procedure described in the next section.

8.2 CONTROL OF SUSPICIOUS TRANSACTIONS

In order to identify suspicious or unusual transactions Ereus will put in place permanent controls over the activities of its customers. There are two types of controls of the transactions:

8.2.1 Decentralized

All employees at Ereus must, while attending to their day-to-day business practices, be alert to detect and report any unusual activity that might arise.
All employees must pay attention to any Red Flags that might come up during the transactions or activities of the customers they attend to. They must verify the transactions carried out by their customers in order to detect those that seem unusual either due to their volume, type of operation, reiteration or lack thereof.
If they do find unusual transactions, staff must fill out an "Internal Operation Report" (See Annex 5), and enclose all the supporting documentation and evidence of their analysis.
This report will be sent to the Compliance Officer. (See 8.4 Investigations)
Section 8.3 lists the main Red Flags Ereus considers in the running of their business.

8.2.2 Centralized

The Compliance Officer must monitor the transactions carried out by customers in order to spot any unusual activity that might occur.
In order to do so, a scheme of Red Flags and Controls has been defined, based on the customer's risk rating and certain predefined follow-up parameters.

8.3 RED FLAGS

8.3.1 Red Flags for Decentralized Monitoring

Red Flags are those behaviors or characteristics of the financial transactions carried out by customers that might help us detect a Suspicious Transaction of money laundering and/or terrorist financing.
Red Flags show us certain behaviors of the customers and unusual situations during a transaction that might be an attempt to conceal money laundering activities. It must also be noted that not all transactions that present unusual or atypical behaviors are illegal activities. An "unusual" transaction might, after being carefully evaluated, show that the customer is conducting perfectly legal operations. In order to determine what is unusual about a transaction, it is necessary to understand its complexity, amount, design, reiteration, if it serves no evident financial, business or legal purpose, based on the characteristics and business-financial profile of the customer.
In summary, there could be many elements that make a transaction suspicious, but in order to evaluate it and prevent from reaching that status, it is of utmost importance the comprehensive knowledge the Institution has of its customer, and the information the customer can submit to explain and validate the origin and purpose of such transaction.
Considering the Estonian Financial Supervision Authority ("EFSA's and international Best Practices' recommendations we can mention the following as behaviors to look for that might trigger Red Flags.
An "Internal Operation Report" must be filled out in the event of a Red Flag (See Annex 4), and all the supporting documentation and evidence of the analysis should be enclosed.
This report will be sent to the Compliance Officer. (See 8.4 Investigations)

A) Cash Transactions
1. Transactions that involve forged or dubious instruments (*)
2. Using cash for a transaction that has not been recounted. When it comes to recounting the funds, the transaction is completed by reducing the amount to $. Currency exchange transactions conducted on behalf of a customer by a third party, and after the transaction is completed, these funds are transferred to locations that bear no evident business connection to the customer or to locations that are considered as non-cooperative.
3. Customers who try to conduct a transaction by using cash or other monetary instruments but withdraw the application after learning about the reporting requirements (*)

B) General Transactions
1. When customers refuse to provide the financial information requested by Ereus during the initial application process. When customers try to conceal or limit the amount of information provided or when they provide false or information that is difficult to verify.
2. Customers who are sent large amounts of money from abroad that is inconsistent with their activities.
3. Company representatives that avoid direct contact with Ereus.
4. Customers who frequently receive funds from so-called "tax havens" or from countries that are considered non-cooperative by FATF, or if they send large amounts of money to these countries on a regular basis.
5. Legal person or organization that have the same address and the same people with authorized signature as other companies and organizations, without there being financial or

legal explanations for such arrangement (for example, people who hold senior positions in several companies located in the same area). Special attention should be paid if any of this companies or organizations are off-shore entities located in tax havens.
6. When a company has different people with authorized signature but there is no apparent relationship between them (whether business or family ties). Special attention should be paid when these are off shore companies located in tax havens.
7. Entity, foundation, association or mutual that conduct transactions of amounts that exceed their regular or habitual income, without there being legal or financial explanations, based on their declared activity and customer profile.
8. Customer referred by a foreign bank located in a country where there is a reportedly high drug trafficking activity or known connections to terrorist organizations, or a country that is considered as non-cooperative to combat money laundering, or a country that is not compliant with international standards (*).
9. Legal person involved in the activities of an association or foundation that is connected to the demands and claims of a terrorist organization.
10. Legal person, foundation or association that might have ties to a terrorist organization and conducts transactions over their estimated income level.
11. Customers that seem to be acting on behalf of a third party but do not want to reveal the true identity of the beneficiary owner.
12. A customer who conducts transactions to and from jurisdictions considered non cooperative, when there seems to be no logical business explanation to conduct such transactions.
13. Customer who sends or receives large fund transfers on a regular basis that cannot be clearly identified as a legitimate transaction, to or from countries where there is a reportedly high drug trafficking activity or known connections to terrorist organizations, or a country that is considered as non-cooperative to combat money laundering, or a country that is not compliant with international standards regarding client identification and Know Your Customer policies (*).

C) Transactions with foreign countries
1. Electronic transfers that do not have sufficient data to trace back the transaction.
2. Transfers where the sender or beneficiary is a foundation, association or other non-profit organization that cannot provide a valid explanation of the source of the funds.
In addition, the origin of the funds must be consistent with the declared activity stated in the Customer Profile.
3. Transfers broken into smaller amounts of money that are clearly trying to avoid a sum of $.
4. Transfers sent or received that do not provide clear information about the sender or payee in order to identify such transaction.
Transfers of large amounts of money to or from abroad that are to be paid in cash.
5. Customers referred by a branch, subsidiary or foreign bank with headquarters in countries or locations considered as tax havens or non-cooperative according to the FATF (*)
6. Customers who send or receive payments on a regular basis and in large amounts, including telegraphic transfers, to or from countries considered as “tax havens” or non-cooperative according to the FATF.

7. International transactions to customers/accounts without having the necessary background on those transactions, or where the stated business activity of the customer does not explain such transaction.
8. Any type of operation in which the customer refuses to provide the standard information requested, if they provide limited information or fake or that it is hard to verify for the institution.
9. Transactions received from locations suspected of money laundering activities.
10. Transfers received from abroad that are almost immediately used for buying financial instruments to conduct payments to third parties.

D) Other Factors

1. Staff at Ereus who show a sudden change in their lifestyle or refuse to take time off.
2. Staff at Ereus who use their personal address to receive documentation from Customers.
3. Special attention should be paid to staff at Ereus who show a sudden and significant increase in their operations.
4. When dealing with PEPs, special attention should be paid to their transaction, making sure these are consistent with the activity stated and their customer profile.
5. If the Entities suspect or have reasonable evidence to suspect of the existence of funds that have ties to terrorism, terrorist acts or terrorist organizations, they should immediately inform that Financial Information Unit. The UN Security Council Resolutions for the Suppression of the Financing of Terrorism will be considered when handling these matters.
6. Customers who make unsound use of the services of Company name.
7. Legal persons owned by individuals of the same origin or with participation of individuals of the same origin from jurisdictions that are considered as non-cooperative.
8. When the customer's phone has been disconnected.

Employees of Company name, that detect any of the behaviors aforementioned, must immediately report them by filling out the Internal Operations Report Form (See Annex 4).

8.4 INVESTIGATIONS

8.4.1 Compliance Officer

The Compliance Officer must conduct an investigation when:

- Customers are listed in the OFAC watch list or as "Unwanted Customers".
- Red Flags are triggered as a result of centralized monitoring.
- An Internal Operations Report is submitted to them as a result of decentralized monitoring.
- They considered it is necessary.

The procedure will be as follows:

The Compliance Officer will conduct the pertinent investigations aided by the business platforms if necessary.

The Compliance Officer will fill out the Unusual Operation Investigation Form (See Annex 5) indicating their recommendations for each case (issuing or not an STR).

If the Compliance Officer considers that the transaction:

• could eventually develop as a money laundering and terrorist financing offense.
• is unusual according to the customs and practices, or is not consistent with the type of operation, frequency or volume the customer usually conducts, and can't find a reasonable financial or legal explanation after examining the facts, including the customer's background and possible purpose of the transaction.
Then the Compliance Officer will present the Committee for the Prevention of Money Laundering and Terrorist Financing the proposal to report the transactions considered suspicious before the UIAF.
The Committee, based on the evidence collected during the investigation, will determine whether or not to report these transactions before the UIAF. If they decide one transaction is not to be considered suspicious, they must properly document and justify this decision.
The Compliance Officer will also inform the Committee about the list of transactions investigated during the process but that were finally cleared.
The Committee for the Prevention of Money Laundering and Terrorist Financing will determine whether or not to continue the relationship with the customer that was subject to the STR.
The decision will be taken under instructions provided by the EFSA.
If after 10 working days from the time the EFSA was presented with the STR, there is no reply against it, then The Committee will proceed as they deem fit.
If the relationship with the customer is terminated, then the Estonian Financial Supervision Authority ("EFSA) shall be notified. If the decision is to continue the relationship with the customer, the Committee might establish specific follow-up guidelines for the case.
If the Committee decided to terminate the relationship with the client, the Compliance Officer shall inform the Account Manager or Branch Manager to proceed with the closing of accounts. This customer will be added to the "Unwanted Customers" list.

8.5 SUSPICIOUS TRANSACTIONS REPORT (STR)
The STR will include the information requested by the UIAF and all the information that is considered relevant to the cause. For those cases in which the Committee decides in favor of issuing and STR, the Compliance Officer is the one responsible for presenting this report before the UIAF in timely form and manner.

8.6 RECORD KEEPING
The following information must be kept, in case it is ever requested by the Regulatory bodies or Justice:
• Documentation necessary for the Identification and/or Know Your Customer policies.
This information will be kept for a minimum of 10 years after the relationship with the customer ended.
• Original documentation or certified copies, for a minimum of 10 years since the execution of the transactions or operations.
• Unusual Operations Report and all supporting documentation, for 10 years after these were issued.
• A copy of every STR issued, together with the supporting documentation, for a minimum of 10 years since the date of the report.

8.7 CONFIDENTIALITY

Authorities and Staff are under express prohibition to disclose the fact that information has been sent to or requested from the Estonian Financial Supervision Authority (“EFSA to any person involved or connected to the suspicious transaction report or to any third party, nor shall they make any reference whatsoever about the case. Any actions taken connected to the prevention of money laundering shall be treated with utmost reserve and confidentiality.

Since STRs are confidential, no copies of the reports will be kept in the file of the customers involved. It is the Compliance Officer’s responsibility to set further safeguards to ensure compliance with the confidentiality policy.

Those who do not comply will be subject to strict disciplinary measures and/or to any criminal sanctions that may apply.

9. “KNOW YOUR EMPLOYEE POLICY”

Ereus bestows trust upon their staff and is confident that they will conduct their business with a strong ethical commitment, honesty and qualified professional expertise.

9.1 KNOW YOUR EMPLOYEE POLICY IMPLEMENTATION

9.1.1 Hiring and Recruiting Staff (External Hiring)

As part of the recruiting and Know Your Customer processes, the company will request the following documentation:

• CV

• Personal and/or Professional background

The company will conduct a personal, professional and financial background check of the candidate when considering their application.

Supervisors/bosses and managers must know the staff in their department and report any substantial change in the financial situation or in the spending habits of the employees working directly under them.

At the same time, the Compliance Department must control that the name of the applicant or employee is not listed in the OFAC, PEPs and/or “Unwanted Customers” watch lists.

Every person in Company name’s payroll will be screened against these lists annually.

9.1.2 Monitoring Employee Behavior

In order to ensure the integrity of Company name’s payroll, supervisors must monitor their staff’s behavior so as to identify and report any situations that might be considered suspicious.

The following are examples of situations to watch out for:

• Sudden and significant changes in their standard of living.

• Lifestyle and spending habits that aren’t consistent with their salary, financial position or level of indebtedness.

• If employee refuses to take time off for no apparent reason.

• Employees who don’t allow other colleagues to assist certain customers.

• If employee suspiciously receives gifts or gratuities on a regular basis.

• Employees who are reluctant to accept any promotions or changes in their activities.

• Employees who stay at the office after working hours or that go to the office at odd times for no reasonable explanation.

Supervisors will be responsible for detecting these behaviors and changes in their employees' conduct and reporting them to the Compliance Officer.
In addition, unusual activities in operations on behalf and to the order of employees will be identified through the Entity's monitoring process, and will be evaluated based on the profile and remuneration of the employees.

9.2 PERFORMANCE EVALUATION, REWARDS AND DISCIPLINARY MEASURES

Due diligence in the compliance with standards for the prevention of money laundering will be considered as yet another element to be evaluated when appraising employee performance. Noncompliance to the Prevention Against Money Laundering and Terrorist Financing Policies is detrimental to Ereus, authorities, officers and employees. Since the reputation of its staff is directly link to the reputation of the company, any infringement will have a double impact. In addition, any breach or infringement of the Prevention Against Money Laundering and Terrorist Financing Policies will mean that staff might be subject to internal disciplinary measures and that Ereus, authorities and officials may be subject to penalties.

10. STAFF TRAINING POLICY

Ereus believes that creating a compliance and control culture among its employees is the best tool to combat money laundering.
Therefore, there's an ongoing effort to promote staff training, development and awareness programs around the many aspects that comprise the laundering of criminal proceeds and terrorist financing.

10.1 INDUCTION COURSE

This course aims to inform newly hired employees about the policies and procedures related to the prevention against money laundering as well as raising awareness about the risks for the institution being used for the fulfillment of these illegal purposes. This course must be conducted within 60 days of the date of beginning of employment.

10.2 PERIODIC COURSES (ON SITE AND/OR ONLINE)

There will be at least one course a year, for all Ereus employees to attend.

10.3 COURSES ABOUT "UPDATES IN REGULATIONS"

Staff must always be updated about existing regulations. In order to do so a course will be conducted every time the Compliance Officer and the Legal Consultant in the Compliance Department deem it necessary.

10.4 COURSE SUBJECTS

Staff in our Company will be trained in the following areas:

• Trends in the prevention of money laundering
• Domestic legal framework and regulations
• Client Identification Program
• Know Your Customer Program
• Customer's Risk Profile
• Decentralized Monitoring of Transactions
• Unusual/Suspicious Transactions Report
• Money laundering and Terrorist Financing Methodologies

The aforementioned are mandatory courses for staff,If possible staff will be tested on these areas to evaluate understanding and knowledge acquisition. The certificate of attendance and test results will be filed in the employee's dossier.
The Compliance Department will keep record of all training courses conducted as well as the staff that attended and obtained passing marks.

The Compliance Officer and the Legal Consultant in the Compliance Department will attend at least one training course a year conducted by a third party, independent from Ereus.

11. ORGANIZATIONAL STRUCTURE

In order to be able to comply with the policies set forth in this manual and with the requirements of the EFSA regarding the prevention against money laundering and terrorist financing, the following structure has been set up:
• Committee for the Prevention of Money Laundering and Terrorist Financing
• Compliance Officer
• Assistant to the Compliance Officer

11.1 COMMITTEE FOR THE PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING

The Committee must promote, facilitate and monitor compliance to the existing legal framework and domestic regulations regarding the Prevention of Money Laundering and Terrorist Financing.
It works as a collegiate body responsible for planning, coordinating and safeguarding the compliance policies established in the "Program for the Prevention of Money Laundering and Terrorist Financing" (herein "The Program").
The Committee will have full access to any and all information and/or documentation they deem necessary in order to fulfill their duties. Depending on the characteristics of each individual case, the Committee might decide to hire an external consultant or expert when they consider it necessary to fulfill their responsibilities.

11.1.1 Purpose and Responsibilities

• To report annually (through the Compliance Officer) to the Board of Directors regarding compliance to The Program, suggesting any pertinent modifications to it.

• To provide oversight and promote the implementation of the Program against Money Laundering and Terrorist Financing and compliance to it.
• To analyze the Internal Operations Reports submitted by the Compliance Officer, in order to approve or dismiss relaying it to the regulatory body (EFSA).
• 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.
• To decide on enhancements to the monitoring and control measures suggested by the Compliance Officer regarding the prevention of money laundering.

11.1.2 Membership and re appointment
The members of the Committee are:
• Company Directors
• Compliance Officer
• Assistant to the Compliance Officer

When the nature of the issues to be discussed so requires, the Committee might decide to call on any other person in Ereus' payroll they consider necessary as well as external consultants who can provide their counseling, knowledge and expertise.

11.1.3 Operation
• The Committee shall hold meetings every two months. They shall hold extraordinary meetings at the request of the Board or Compliance Officer.
• The quorum required to conduct the meeting is 2 people.
• Decisions will be taken by straight majority vote.
• The Committee can decide to call on any person in the company's payroll to assist in their operations.
• The Committee can decide to issue an STR by email, there's no need to physically meet.
The Compliance officer is the member responsible for keeping record of these decisions, and these
(emails) will be authenticated in writing at the following meeting the Committee holds.
• The Committee will keep minutes of its meetings.

11.2 COMPLIANCE OFFICER
Following regulations of the Estonian Financial Supervision Authority ("EFSA"), the position of Compliance Officer has been created. This is a management position held by a person of trust.
The Compliance officer will not be part of the Internal Audits department at Company name.
The Compliance Officer will have full access to any and all information and/or documentation they deem necessary in order to fulfill their duties.
They will be supported by staff in the "Compliance Department".

11.2.1 Purpose and Responsibilities
• To implement the "Prevention against Money Laundering and Terrorist Financing" program.
• To monitor transactions carried out by customers.
• To investigate reports of unusual transactions, as well as those detected in the centralized

monitoring process.
• To submit to the Committee those transactions considered suspicious to confirm that status and decide if these will be reported.
• To keep record of the unusual transactions reported by staff, as well as those detected in the centralized monitoring process.
• To keep record of STRs, as well as statistics of the STRs issuance to be discussed at Committee meetings.
• To verify and make sure records are properly kept and safely guarded to prevent laundering of assets.
• To present before the Committee suggestions to improve or implement new procedures for the Prevention against Money Laundering Program.
• To present before the Committee any changes they deem pertinent in the methodology to rate customer risk.
• To set up staff training courses.
• To keep informed and updated about all legal matters and regulations that affect Ereus in their management of the prevention against money laundering.
• To liaise with independent consultants who might be investigating or monitoring compliance to regulations.
• To inform the committee about any requests by Regulatory Bodies, Auditors and Consultants.
• To implement the necessary remedial measures as a result of observations made by the Internal or External Audit or Regulatory Body.
• To liaise with EFSA to provide all the information they request when a suspicious transaction has been reported.
• To send STRs to the EFSA when approved by the Committee.
• To inform the Board when an STR has been issued. The Board must be formally acknowledged.
• To enforce standards and procedures for the Prevention of Money Laundering and Terrorist Financing.

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

The appointment of the Compliance Officer will be informed to the EFSA (detailing name, position and branch).

If there are any changes or updates to this information, the EFSA must also be notified, within 5 days after the Officer was appointed.

12. INDEPENDENT AUDITS

EXTERNAL AUDITS

Six months after the end of the fiscal year, following the established procedures, the company will submit before the Estonian Financial Supervision Authority (“EFSA”) an annual report

issued by external auditors. This report evaluates the policies and procedures of the existing Prevention Program. The auditor must express their views regarding the appropriateness and efficiency of the policies and procedures the institution has adopted as protection from being used as a means to launder illegally obtained funds and finance terrorism. The report must also indicate any significant deficiencies or weaknesses as well as the remedial measures suggested and finally adopted.

13. FINANCIAL TRANSACTIONS REPORT

Ereus must inform the Estonian Financial Supervision Authority (“EFSA”) about natural or legal persons who carry out transactions that consist of the conversion of national or foreign currency into crypto currency or other easily convertible securities in amounts over USD 10,000 (ten thousand US Dollars) or equivalent in other currencies. Ereus should also report transactions carried out by one single natural or legal person that over the course of one month amounts to over USD 10,000 (ten thousand US Dollars).
The information aforementioned must be sent to the Estonian Financial Supervision Authority (“EFSA”) so it is entered into the centralized database. Instructions on how to do so will be provided when needed.

14. TRANSFERS, PROCEDURES AND POLICIES

14.1 REQUIREMENTS FOR TRANSFERS

Records shall be kept including the following information:

14.1.1 Transfers issued by Company name

The following information is required to issue transfers:
• Transferor’s full name and last name
• Transferor’s address
• Reference Number (or account number)
• Amount
• Date
• Payment instructions
• Identity of beneficiary entity
• Name of Beneficiary
• Beneficiary’s account number
• If applicable: beneficiary’s address

A copy of the transferor’s ID card must be kept.

A file with all the information and documentation submitted must be kept for at least 5 years.

Enhanced Due Diligence

When transfers issued to the same beneficiary go over USD 10,000 a month, the following additional documentation and information will be requested:

Beneficiary Legal Person
Conduct an Internet search for information on the company and its business activity (activity, location, background), checking for consistency with transferor's information.

14.1.2 Crypto Transfers received by Ereus

- Clients are required to register a Ereus Account in order to have access to the Ereus Platform.
- Clients are required to complete the KYC process supplying the following information:
- Full name and proof of identity
- Full address and proof of residency.
- They are to certify that the information you have to provide to Company name, including during registration and during the KYC process, is accurate and complete.

14.1.3 Fiat Transfers received by Ereus

A copy of the bank's credit notice shall be kept.

The following information must be submitted by the transferor financial institution:
• Transferor's full name
• Transferor's address
• Transferor's account number or identification number at financial institution
• Identity of transferor entity
• Amount
• Date
• Name of beneficiary
• Beneficiary's ID or passport number
When dealing with an occasional customer and the funds are withdrawn in person, the identity must be verified and request the following information:
• Name and address
• Type of identification verified
• Number of identifications presented
• Tax payer registry number

The information must be kept for 5 years and should be accessible by the name of the beneficiary.

No funds will be transferred to anonymous accounts, numbered accounts or under fictitious or nonexistent names.

ANNEX 1 – HIGH RISK GEOGRAPHIC LOCATIONS

• As of 21 Feb 2020 only Iran and the Democratic People's Republic of Korea hold the High Risk profile according to FATF
• The members of FATF or regional groups of similar nature are the following:
Argentina
Aruba
Australia
Austria
Belgium
Brazil
Canada
China
Cooperation Council of the Gulf
Denmark
Dutch Antilles European Commission Finland
France
Germany
Greece
Hong Kong,
China
Ireland
Island
Italy
Japan
Luxemburg
Mexico
New Zealand
Norway
Portugal
Russia
Singapore
South Africa
Spain
Sweden
Switzerland
The
Netherlands
Turkey
UK
USA

APG (Asia/Pacific Group on Money Laundering)
Afghanistan

Australia
Bangladesh
Brunei Darussalam Cambodia
Canada
China
Cook Islands
Fiji Islands
Hong Kong,
China
India
Indonesia
Republic of Korea (South Korea)
Japan
Macao, China
Malaysia
The
Marshall
Islands
Mongolia
Myanmar
Nepal
New
Zealand
Niue
Pakistan
Palau
The Philippines
Samoa
Singapore
Sri Lanka
Thailand
Tonga
United States of America
Vanuatu

FATF ASSOCIATE MEMBERS

Albania
Andorra
Armenia
Azerbaijan
Bosnia and Herzegovina
Bulgaria
Croatia
Cyprus

Czech Republic
Estonia
France
Georgia
Hungary
Latvia
Liechtenstein
Lithuania
Malta
Moldova
Monaco
Netherlands
Poland
Rep. of Macedonia
Romania
Russia
San Marino
Serbia
Slovakia
Slovenia
Ukraine

GAFISUD (Financial Action Task Force on Money Laundering in South America)
Argentina
Bolivia
Brazil
Chile
Colombia
Ecuador
Paraguay
Peru
Uruguay

MENAFATF (Middle East and North Africa Financial Action Task Force)
Algeria
Bahrain
Egypt
Jordan
Kuwait
Lebanon
Morocco
Oman
Qatar
Saudi Arabia

Syria
Tunisia
UAE
Yemen

EAG (Eurasian Group)
Belarus
China
Kazakhstan
Kyrgyzstan
Russia
Tajikistan
Uzbekistan

ESAAMLG (Eastern and Southern Africa Anti-Money Laundering Group)
Botswana
Kenya
Lesotho
Malawi
Mauritius
Mozambique
Namibia
South Africa
Swaziland
Seychelles
Tanzania
Uganda
Zambia
Zimbabwe

FATF OBSERVERS

GIABA (Intergovernmental Action Group against Money Laundering in Africa)
Benin
Burkina Faso
Cape Verde
Côte d'Ivoire
Gambia
Ghana
Guinea
Guinea Bissau
Liberia
Mali

Niger
Nigeria
Senegal
Sierra Leone
Togo

CFATF (Caribbean Financial Action Task Force)
Anguilla
Antigua and Barbuda
Algeria
Aruba
Bahamas
Barbados
Belize
Bermuda
British Virgin Islands
Cayman Islands
Costa Rica
Dominica
Dominican Republic
Dutch Antilles
El Salvador
Grenada
Guatemala
Guyana
Haiti
Honduras
Jamaica
Montserrat
Nicaragua
Panama
Saint Kits and Nevis
Saint Vincent and the Grenadines
St. Lucia
Suriname
Trinidad and Tobago
Turks and Caicos
Venezuela

Not Members of Any Group
Angola
Bhutan

Burundi
Cameroon
Central African
Republic Chad
Comoros
Congo
Cuba
Democratic Republic of Congo
Djibouti
East Timor
Equatorial
Guinea
Eritrea
Ethiopia
Gabon
Iraq
Iran
Israel
Kiribati
Laos
Libya
Madagascar
Maldives
Mauritania
Micronesia
Montenegro
North Korea
Papua
New Guinea
Rwanda
São Tomé and Príncipe
Solomon Islands
Somalia
Sudan
Taiwan
Turkmenistan
Tuvalu
Vanuatu
Vatican
Vietnam

ANNEX 2- CUSTOMER RISK RATING

a) Is the customer a Politically Exposed Person, or does he/she have any substantial connections to one?
Yes / No
If yes, indicate name and type of connection
_____
_____
_____

b) Does the customer have any substantial connection to a high-risk geographic location?
Yes / No
If yes, indicate geographic location and type of connection
_____
_____
_____

c) Does the customer have a substantial connection to a high-risk activity?
Yes / No
If yes, indicate type of activity and type of connection
_____
_____
_____

d) Materiality
Estimated AUMs in the next 12 months
USD 30,000 – USD 100,000 / USD 250,000 – USD 500,000 / USD 100,000 – USD 250,000 / over USD 500,000
_____
_____
_____

Additional Comments – Customer relationship background
_____
_____
_____
_____
_____

AML Risk Rating: LOW / MEDIUM / HIGH

Authorizing Officers:
Name and Signature: _____
Compliance Officer's Signature: _____
Date: _____

ANNEX 3 – IDENTIFICATION FORM

NATURAL PERSON

Full Name and Last Name: _____
Identity Document Type: _____ Number: _____
Issuing Country: _____ Expiry: _____
Place and Date of Birth: _____
Spouse's Name and Last Name: _____
Identity Document Type: _____ Number: _____
Home Address: _____
City: _____
Telephone/Fax Number: _____
Email: _____
Personal/Bank References
Names:

_____
Telephone Number:
_____ Address:

_____
Persons Authorized to Operate (same information as account holder)
I hereby declare, under this sworn statement, that all the information provided is accurate and true and that I will inform Ereus of any changes it might suffer. I also declare, under this sworn statement, that the funds I shall operate with are of legal origin and that these funds are not the proceeds or illegal activities conducted by me or third parties.
Customer's signature: _____ Date: _____

LEGAL PERSON

Corporate name: _____
Type of business entity: _____
Identification Number: _____
Country of incorporation: _____
Date of incorporation: _____
Legal address: _____
Main business activity: _____
Email: _____
Telephone/Fax Number: _____
Personal/bank references:
Names: _____
Telephone Number: _____
Address: _____
Identification of persons authorized to operate/ shareholders/ Beneficiary Owner (same information as natural persons)

(*) Enclose copy of document

Enclose:

- Certified copy of the articles of incorporation or bylaws
- Copy of taxpayer registry
- Copy of the power of attorney, certified by notary public, given to the natural person that will conduct the transactions or authorized representatives or authorities.

I hereby declare, under this sworn statement, that all the information provided is accurate and true and that I will inform Ereus of any changes it might suffer. I also declare, under this sworn statement, that the funds I shall operate with are of legal origin and that these funds are not the proceeds
or illegal activities conducted by me or third parties.

Customer's signature: _____ Date: _____

ANNEX 4 – INTERNAL OPERATION REPORT

Ereus CUSTOMER IDENTIFICATION – Legal Person

Corporate Name
Address Tax Registry Number Telephone Numbers
Main Business Activity:

CUSTOMER IDENTIFICATION – Natural Person

Last Names: First Names:
Address ID Tax Registry Number
Nationality DOB Telephone Number

Unusual transaction details

Date of unusual transaction
_____/_____/_____

Amount involved in the unusual transaction

What was unusual about the transaction:

Other background information (state dates, amounts, suspicious behaviors of the customer and any other information you consider relevant to explain why the transaction(s) was/were unusual. If necessary, attach papers for more space).

Information Complied by:

Last Names First Names
Position/Title Signature Date __/__/__

Compliance Officer

Last Names First Names
Position/Title Signature Date __/__/__

Recipient Date of Reception Dispatch Date

_____/_____/_____ _____/_____/_____
_____/_____/_____ _____/_____/_____

Important: once the form has been filled out it cannot be photocopied and it must be submitted in a closed envelope, marked Confidential, to the Compliance Officer, **no longer than 5 days after the unusual transaction was detected.** Confidentiality is required.

ANNEX 5 – INVESTIGATION OF INTERNAL OPERATION REPORT (IOR)

Company name
Identification of customer, potential customer or any person that has conducted or has tried to conduct unusual transactions.
Name/Corporate Name
Tax Payer Identification Number
Account Executive (If applicable)
Transactions conducted by customer in the past 12 months
Type of transaction # Amount Counterpart (if applicable)
Account Executive's Comments
Outcome of the Investigation Conducted

Recommendation to the Committee	Explanation
DON'T Issue IOR	
DO Issue IOR	
Investigate further	

Compliance Officer Signature

Date

ANNEX 6 –SUSPICIOUS TRANSACTION REPORT PARTICULARS OF COMPLAINANT

Name of Complainant Entity: Ereus
Type of Entity: Crypto Exchange
Address:
Contact Person
First Name and Last Name: _____
Title/Position: _____
Telephone Number: _____
E-mail: _____
TRANSACTION REPORTED - SUBJECTS
Name/Corporate Name: _____
_____
Tax Registry Number: _____
Type and Identity Document Number: _____
Nationality: _____Date and Place of Birth: _____
Spouse's Last Name: _____
Address: _____
Connection to the event reported (Direct, Indirect, Partner, Representative, etc.):
Tax Registry Number: _____
Type and Identity Document Number: _____
Nationality: _____Date and Place of Birth: _____
Spouse's Last Name: _____
Address: _____
Connection to the event reported (Direct, Indirect, Partner, Representative, etc.):

TRANSACTION REPORTED
Date or period when reported transaction was conducted:
_____

Description of the reported transaction:

Signature:

Print Name:
Date