

Corporate Policy for the Prevention and Fight against Money Laundering

01.2022

1. PURPOSE

The Corporate Policy for the Prevention and Fight against Money Laundering, Terrorist Financing and Concealment of Assets, Rights and Securities in Operations ("Policy") aims at establishing the guidelines and rules that must be observed by all members and associates of Alaska Inverimentos Ltda. ("Alaska" or "Manager"), with the purpose of promoting the alignment of operational activities with legal and regulatory requirements, as well as the international best practices relevant to the crime of Money Laundering, Terrorist Financing and Concealment of Assets, Rights and Securities (PLD/CFT/OBDV).

2. PERIOD OF VALIDITY

This Policy must be reviewed and approved by the Compliance Officer and the Executive Committee, on an annual basis or at a later date, if so requested by the regulatory agency.

Once approved by the Compliance Board and Executive Committee, this Policy will be widely disclosed internally and will be made available on its website and Intranet.

3. GENERAL PROVISIONS

3.1 INTRODUCTION

It is the responsibility of all members and associates, especially professionals related to the Alaska's distribution area, to know and understand the terms of this Policy and seek to prevent and detect operations or transactions that have atypical characteristics in order to fight crimes of Money Laundering, Terrorist Financing and Concealment of Goods, Rights and Securities.

The laws and regulations related to these offenses, as well as the rules and guidelines established by this Policy, must be mandatorily complied with.

This Policy identifies concepts of Money Laundering and Terrorist Financing, the stages that shape the offense and the characteristics of people and products susceptible to the involvement with this crime. The Policy also reinforces the commitment of the entire organizational structure to fighting Money Laundering and Terrorist Financing.

Knowledge of any evidence of Money Laundering and Terrorist Financing or other illegal act must be reported to the Compliance area, which is responsible for investigating the reported information and, if applicable, communicating it to regulatory agencies.

3.2 DEFINITIONS

- Money Laundering: The term "money laundering" is the practice of criminal activities intended to turn illicit money into licit, that is, it is the process by which the criminal transforms resources earned in illegal activities into resources with an apparently legal origin, to conceal or disguise the nature, source, location, disposition, movement or ownership of goods, rights or securities originating directly or indirectly from a criminal offense.
 - Terrorist Financing: Consists of the collection of funds and/or capital for the conduct of terrorist activities. These funds may come from donations or gain from various licit or illicit activities such as drug trafficking, prostitution, organized crime, smuggling, extortion, kidnapping, fraud, etc.
 - Corruption: Consists of suggesting, offering, submitting, requesting, accepting or receiving, directly or indirectly, from people of the public, private or third sector organizations, undue advantages.
- Politically Exposed Person (PEP): A politically exposed person is deemed to be public agents who hold or have held, in the last five (5) years, in Brazil or in foreign countries, territories and

dependencies, relevant public positions, jobs or activities, as well as their representatives, family members and other people with a close relationship. In addition, they are examples of situations that characterize close relationship and lead to the classification of the client as a politically exposed person, as direct or indirect control, of a legal entity client.

- Final Beneficiary: It is the person who ultimately, directly or indirectly, owns, controls or significantly influences the business structure. Except for legal entities incorporated as a publicly-held company or non-profit entity and cooperatives, for which the information collected must cover the information of individuals authorized to represent them, as well as controllers, managers and officers, if any.

3.3 STAGES OF THE CRIME OF MONEY LAUNDERING

The process of Money Laundering involves three stages, which are: placement, concealment and integration.

Placement is the stage in which the criminal introduces the illicitly obtained values into the economic system through deposits, purchase of negotiable instruments or purchase of goods. It deals with the removal of the money from the location that it was illegally acquired and its inclusion, for example, in the financial market.

Concealment is the moment when the agent conducts suspicious transactions characterizing the crime of Money Laundering. This stage consists of the physical segregation between the agent and the illicit money through several complex transactions to disassociate the illegal source of the money.

During integration, the illegal resource definitely integrates the economic and financial system. As of this moment, the money appears to have derived from a lawful origin.

4. ROLES AND RESPONSIBILITIES

The entire Alaska's organizational structure has specific responsibilities in fighting Money Laundering and Terrorist Financing, as described below:

Executive Committee

- Approve corporate standards, measures and guidelines related to the PLDCFT;
- Be aware of the assignments for operational areas directly affected by the PLDCFT rules, with the designation of related responsibilities;
- Monitor the effectiveness of activities and actions related to the PLDCFT;
- Ensure compliance with all rules and procedures established by the Policy and manuals related to the PLDCFT;
- Assess the reports and communications issued by regulatory agencies, self-regulating agencies, internal and external audit, determining the actions and measures necessary to meet the demands;
- Resolve on the hiring of specialized professional services, investments in control systems and technology, when deemed convenient;

OFFICER RESPONSIBLE FOR PREVENTING AND FIGHTING CRIMES OF MONEY LAUNDERING AND TERRORIST FINANCING

- Implement and monitor compliance with this Policy, other standards and their updates; and
- Comply with the provisions of the regulatory agencies to act in the PLDCFT.

COMPLIANCE

- Resolve on guidelines applicable to the issues of Preventing Crimes of Money Laundering and Fighting Terrorist Financing ("PLDCFT");

- Implement and update policies and standards relevant to preventing and fighting crimes of Money Laundering and Terrorist Financing;
- Ensure compliance with the national legislation, standards, regulations and policies governing the prevention and fight of crimes of Money Laundering and Terrorist Financing;
- Disseminate and act as a multiplier of the culture for the prevention and fight against crimes of Money Laundering and Terrorist Financing;
- Develop and implement tools and processes to support corporate program strategies in order to prevent Money Laundering and Terrorist Financing;
- Ensure that the acceptance of clients, from the perspective of PLDCFT, is conducted while mitigating exposure to reputational risks, ensuring the identification of PEPs and clients in "Special Attention" situation;
- Interact with regulatory agencies;
- Monitor, identify and deal with operations performed by clients under the monitoring rules in order to minimize operational, legal and image risks of Alaska;
- Establish processes and procedures for the identification, monitoring and analysis of suspicious activities and/or operations of money laundering and financing of terrorism, subsidizing the PLD/CFT COMMISSION with the necessary information for the decision-making process;
- Ensure that after due resolution by the Executive Committee, clients, suppliers or business partners who present suspicions of illegal transactions are duly notified to COAF (Financial Activities Control Council), within the regulatory time limit; keep the information of the institution up to date with COAF, providing statements when necessary;

- Implement procedures for the identification, monitoring and reporting, to COAF, of operations of insurance and pension within the reporting criteria established within the applicable regulations.
- Periodically monitor the news disclosed in the media related to Money Laundering and Terrorist Financing and verify the impacts on the list of active clients;
- Previously analyze projects that deal with the development of new products and services, in order to mitigate the risks of such products involving and/or being used for practicing crimes of Money Laundering or Terrorist Financing;
- Pre-analyze new products and services from the perspective of Money Laundering prevention; and
- Develop and maintain, at the disposal of the senior management, audits and regulators, reports and the record of regulatory obligations regarding the PLDCFT, observing the regulatory deadline.
- Establish procedures and internal controls for the identification and treatment of clients, individuals and legal entities or entities subject to sanctions provided for by Law No. 13.810 as of 2019.
- Enable periodic training programs to ensure that all employees and self-employed agents are properly guided and up-to-date regarding their obligations and responsibilities, in due accordance with applicable regulations;

RISK BOARD

- Identify, assess, monitor the operational risk and report to the Compliance if any irregularity is identified; and

DISTRIBUTION BOARD

- Follow the best practices regarding the "Know your Client" process, especially in the acquisition, intermediation, further communicate suspicious activities to the Compliance;

- Comply with internal procedures for identification and maintenance of client records;
- Establish procedures to identify and obtain registry data with the purpose of identifying and knowing the client, as well as ensuring regulatory service;
- Establish controls for validation of registry data declared by the clients;
- Ensure that the client record is in compliance with the Federal Revenue status;
- Fill out the Registration Form correctly and in a timely manner;
- Update the Registry in a period not exceeding the period required by the regulation;
- Consult Compliance when there is evidence of irregularity or doubt as to the procedure to be adopted for the proper referral of the process; and
- Identify clients that are Politically Exposed Persons, clients on restricted lists, clients who reside in a border region or have nationality in a country deemed sensitive for PLDCFT purposes, or who have a background in a risky profession or risky activities, who follow a particular procedure with the implementation of the process only after explicit authorization from the Compliance area;
- Annually, the registration area must conduct a validation test of the registry data of active clients.
- Notify the Compliance if any Conflict of Interest is identified, in order to ensure that the operator performs its activities independently;
- Monitor atypical operations;
- Observe the correct classification of operations;
- Maintain records of transactions based on documents proving their legality;
- Assess whether the operations are in accordance with the operational modality and technical qualification of the client.

4.6 INFORMATION TECHNOLOGY DEPARTMENT

i. Ensure that the PLDCFT systems are properly in operation, ensuring fault resolution in the shortest possible response time.

5. PROCESS TO IDENTIFY AND DEAL WITH EVIDENCE OF MONEY LAUNDERING AND TERRORIST FINANCING

5.1. IDENTIFICATION

Client Identification Process “Know Your Client” or KYC – Know Your Client

This is a set of actions that establish mechanisms to ensure the identification, economic activity, origin and constitution of assets and financial resources of clients, including the collection, updating and filling of registration information, also including specific procedures for the identification of final beneficiaries and Politically Exposed Persons.

Alaska does not admit the opening and maintenance of anonymous accounts. It is prohibited to start or maintain relationships with individuals or entities mentioned in the lists of financial sanctions of the United Nations (UN), US Office of Foreign Assets Control (OFAC) and the European Union.

Alaska adopts, as the primary means for client registration, the electronic client identification form.

The Distribution area is responsible for the analysis, recording of information and documents identification of clients with which the institution maintains a relationship. In order to improve the “Know your Client” process, Alaska develops, in addition to the restricted list research, complementary research activities with regards to the client, such as: requesting additional documentation for clients in risky situations and adopting specific internal procedures. The search on restrictive lists is constituted as a preventive procedure that seeks to signal if the client has been a part in situations of money laundering and terrorist financing.

These routines are intended to identify whether clients are politically exposed persons (PEPs), whether they are on some external restricted list, exercise a risky profession (internal list), and whether they reside in a border city. Regarding the improvement of all practices related to the process of Prevention against Money Laundering and Fight against Terrorist Financing, related to cybercrimes, control is carried out through intelligent software, which validates the data informed by the client, performing analysis of possible document fraud.

When a client has a higher level of risk, a more detailed diligence is conducted in the monitoring processes. Due diligence is conducted so that the institution may identify its clients and verify the information relevant to the conduction of business and transactions, mitigating the risks of financial crimes relevant to digital media.

"Know Your Employee" Process

It is a set of rules, procedures and controls that must be adopted for selection and monitoring of the economic-financial situation and suitability, in order to avoid bond with people involved in illicit acts.

"Know Your Supplier" Process

It is a set of rules and procedures that must be adopted for the identification and acceptance of suppliers and service providers, preventing the hiring of companies that are not in good standing or suspected of involvement in illicit activities. For those who poses a greatest risk, complementary procedures and in-depth assessment diligences and specific competent approval must be adopted, according to the critical nature of the notes or exceptions of the "Know Your Partner" Process.

This is a set of rules, procedures and controls that must be adopted for the identification and acceptance of trading partners, aiming at the prevention of conducting business with counterparties that are not in good standing or suspected of involvement in illicit activities, as well as ensuring that they have adequate PLDCFT procedures, where applicable.

Assessment of New Products and Services

The Compliance area advises the Executive Committee to assess in advance, from the perspective of PLD/CFT, the new products and services in order to mitigate regulatory risks and risks of these products involve and/or be used for the commission of crimes of money laundering or terrorist financing.

Giveaways and Gifts Policy

All giveaways and gifts received by any associate, member or officer of Alaska regarding the performance of their activities in Alaska must be reported to the Compliance Officer, who must assess the relevance and whether the gift may constitute a conflict of interest or in any way interfere with the good practices of Alaska. Giveaways and gifts that do not exceed the amount of five hundred reais (R\$ 500.00) are not included.

5.1.2 MONITORING OF TRANSACTIONS

The Compliance department is responsible for routine monitoring of operations to identify evidence of Money Laundering and Terrorist Financing.

The monitoring is conducted through processes that collect registry information, operational and financial movement of clients, by parameterization of rules.

Once the occurrence is generated, it is up to the Compliance area to analyze the client and its operations in order to confirm the indications of Money Laundering and Terrorist Financing or not.

As a result of any identification of evidence of Money Laundering, corruption or Terrorist Financing by clients, Alaska may decide to block the client's account and/or terminate the relationship.

5.1.3 COMMUNICATION OF SUSPICIOUS TRANSACTIONS TO REGULATORY AGENCIES



Operations, situations or proposals with evidence of money laundering or terrorist financing must be reported to the proper regulatory agencies, where applicable, in compliance with legal and regulatory requirements. The communications in good faith do not incur civil or administrative liability to Alaska, its administrators and associates.

Information regarding communications are restricted, not disclosed to clients or third parties.

5.2 TRAINING

Compliance provides all associates and members with training aimed at reviewing the concepts contained in this Policy and encouraging the adoption of appropriate measures against suspected cases of Money Laundering and Terrorist Financing. Annually, the Compliance reviews the materials and everyone is required to carry out a new training.

5.3 BLOCKING OR TERMINATION OF RELATIONSHIP

As a result of any identification of indications of Money Laundering, corruption or Terrorist Financing by clients, Alaska may decide to block the client's account or terminate the relationship, as well as to possible communicate it to regulatory agencies, as per determination of the Executive Committee.

6. MAINTENANCE OF INFORMATION AND RECORDS

Documents regarding operations, including recordings and registration documents, must be filed for a minimum period of five (5) years from the closing of the account or the completion of the last transaction conducted by the client.

7. CONFIDENTIALITY OF INFORMATION

All information related to evidence/suspicious of money laundering and fight against terrorism financing shall be confidential and shall not, under any circumstances, be disclosed to the parties concerned and may only be reported to the competent agency.

If any associate reports to the Compliance Officer or if the Compliance Officer finds any indication of violation, the Compliance Officer must investigate in secrecy, and may use external advice or report to the competent public administration agency so as not to compromise the investigations.

8. APPLICABLE EXCEPTIONS AND SANCTIONS

For cases of exception to compliance with the rules provided for in this Policy, the applicant must submit an exception request to the Executive Board with the reasons for it, and the approval of the request must be made by at least two officers, whose Policy is applicable.

Penalties Prescribed

Failure to comply with legal and regulatory provisions shall subject associates and members to penalties ranging from administrative to criminal penalties, for Money Laundering, Terrorist Financing and Fraud. Negligence and voluntary failure are deemed non-compliance with this Policy and the Code of Ethics and Conduct, and may be subject to disciplinary measures provided for in the internal regulations.