Effective date: 03/24/2026
Approved by: Risk and Compliance Committee / Risk and Compliance Officers
Minimum review: 24 months
Next scheduled review: 03/24/2028

Anti-Corruption, Anti-Money Laundering and Counter-Terrorist Financing (AML/CFT) Policy, Supplier Engagement (Know Your Partner – KYP), Employees and Know Your Client (KYC)

Alaska Investimentos Ltda.

1. PURPOSE

The Anti-Corruption, Anti-Money Laundering, Counter-Terrorist Financing and Concealment of Assets, Rights and Valuables in Transactions Policy, Supplier Engagement (Know Your Partner – KYP), Employees and Know Your Client Policy ("Policy") aims to define the guidelines and rules to be observed by all partners and employees of Alaska Investimentos Ltda. ("Alaska" or "Manager"), with the objective of promoting the adequacy of operational activities to legal and regulatory requirements, as well as international best practices relevant to the crimes of Corruption, Money Laundering, Terrorist Financing and Concealment of Assets, Rights and Valuables (AML/CFT/CARV), and for the identification of clients, suppliers and employees.

2. TERM

This Policy must be reviewed and approved by the Compliance Officer and the Executive Committee every two years, or within a shorter period, if so required by the regulatory body. Once approved by the Compliance Department and the Executive Committee, this Policy will be widely disclosed internally and made available on its website and Intranet.

3. GENERAL PROVISIONS

3.1 INTRODUCTION

It is the responsibility of all partners and employees, especially professionals linked to Alaska's distribution area, to know and understand the terms of this Policy and to seek to prevent and detect transactions with atypical characteristics in order to combat the crimes of Money Laundering, Terrorist Financing and Concealment of Assets, Rights and Valuables. The laws and regulations linked to these offenses, as well as the rules and guidelines established by this Policy, must be mandatorily complied with. This Policy identifies the concepts of Money Laundering and Terrorist Financing, the stages that constitute the offense, and the characteristics of persons and products susceptible to involvement in this crime. The Policy also reinforces the commitment of the entire organizational structure to combating Money Laundering and Terrorist Financing. Knowledge of any indication of Money Laundering, Terrorist Financing or other unlawful act must be reported to the Compliance area, which is responsible for investigating the reported information and, where applicable, reporting to the regulatory bodies.

3.2 DEFINITIONS

- Money Laundering: The term "money laundering" consists of the practice of criminal activities aimed at turning illicit money into licit money, that is, it is the process by which the criminal transforms resources earned from illegal activities into resources with an apparently legal origin by hiding or disguising the nature, origin, location, disposition, movement or ownership of assets, rights or valuables arising, directly or indirectly, from a criminal offense.
- Terrorist Financing: Consists of gathering funds and/or capital to carry out terrorist activities. These funds may come from donations or be earned from various lawful or unlawful activities such as drug trafficking, prostitution, organized crime, smuggling, extortion, kidnapping, fraud, etc.
- Corruption: Consists of suggesting, offering, submitting, soliciting, accepting or receiving, directly or indirectly, improper advantages, to persons in the public sector, private sector or third-sector organizations. Politically Exposed Person (PEP): Politically exposed persons are considered to be public officials who perform or have performed, in the last 5 (five) years, in Brazil or in foreign countries, territories and dependencies, relevant public positions, jobs or functions, as well as their representatives, family members and other persons closely related to them. In addition, examples of situations that characterize a close relationship and lead to a client's classification as a politically exposed person include direct or indirect control of a corporate client.
- Final Beneficiary: The person who ultimately, directly or indirectly, owns, controls or significantly influences the corporate structure. Excepted from this are legal entities incorporated as publicly held companies or non-profit entities and cooperatives, for which the information collected must cover the information of the natural persons authorized to represent them, as well as controlling shareholders, administrators and officers, if any.

3.3 STAGES OF THE CRIME OF MONEY LAUNDERING

The Money Laundering process involves three stages: placement, layering and integration. Placement is the stage in which the criminal introduces the illicitly obtained funds into the economic system through deposits, the purchase of negotiable instruments or the purchase of goods. It involves removing the money from the place where it was illegally acquired and including it, for example, in the financial market. Layering is when the agent carries out suspicious transactions characterizing the crime of Money Laundering. This phase consists of the physical separation between the agent and the illicit money through various complex transactions in order to disassociate the money from its illegal source. In integration, the illegal funds permanently become part of the economic and financial system. From this point on, the money takes on a lawful appearance.

4. ROLES AND RESPONSIBILITIES

Alaska's entire organizational structure has specific duties in combating Money Laundering and Terrorist Financing, as described below: Executive Committee

- Approve corporate-level rules, measures and guidance related to AML/CFT;
- Be aware of the duties assigned to the operational areas directly affected by the AML/CFT rules, with the designation of the corresponding responsibilities;
- Monitor the effectiveness of the activities and actions related to AML/CFT;

- Ensure compliance with all rules and procedures established in the Policy and in the manuals related to AML/CFT;
- Review the reports and communications issued by regulatory and self-regulatory bodies, internal audit and external audit, determining the actions and measures necessary to meet the demands;
- Resolve on the engagement of specialized professional services and investments in control systems and technology, when deemed appropriate;

OFFICER RESPONSIBLE FOR THE PREVENTION AND COMBATING OF MONEY LAUNDERING AND TERRORIST FINANCING CRIMES

- Implement and monitor compliance with this Policy, the other rules and their respective updates; and
- Comply with the determinations of the regulatory bodies for action on AML/CFT.

COMPLIANCE

- Resolve on the guidelines applicable to matters of Prevention of Money Laundering Crimes and Combating Terrorist Financing (“AML/CFT”);
- Apply and update the policies and rules relevant to the prevention and combating of Money Laundering and Terrorist Financing crimes;
- Ensure compliance with the legislation, standards, regulations and internal policies governing the prevention and combating of Money Laundering and Terrorist Financing;
- Disseminate and act as a multiplier of the culture of prevention and combating of Money Laundering and Terrorist Financing crimes;
- Develop and implement tools and processes to support the strategies of the corporate program for the prevention of Money Laundering and Terrorist Financing;
- Ensure that client acceptance, from an AML/CFT perspective, is carried out while mitigating exposure to reputational risks, ensuring the identification of PEPs and clients in a “Special Attention” situation;
- Interact with regulatory bodies;
- Monitor, identify and handle transactions carried out by clients that fall under the monitoring rules, in order to minimize Alaska’s operational, legal and image risks;
- Establish processes and procedures for identifying, monitoring and analyzing activities and/or transactions suspected of money laundering and terrorist financing, providing the AML/CFT COMMITTEE with the information necessary for decision-making;
- Ensure that, following due resolution by the Executive Committee, clients, suppliers or business partners suspected of illicit transactions are duly reported to COAF within the regulatory deadline; keep the institution’s information up to date with COAF, providing statements when necessary;
- Implement procedures for identifying, monitoring and reporting to COAF insurance and pension transactions that fall under the reporting criteria established in the applicable regulations.
- Periodically monitor news published in the media related to Money Laundering and Terrorist Financing and check the impacts on the list of active clients;

- Analyze in advance the development projects for new products and services, in order to mitigate the risks of such products being involved in and/or used for the practice of Money Laundering or Terrorist Financing crimes;
- Analyze new products and services in advance, from a Money Laundering prevention perspective; and
- Prepare and keep available to senior management, auditors and regulators the reports and the record of regulatory obligations related to AML/CFT, in accordance with the regulatory deadline.
- Establish internal procedures and controls for identifying and handling clients, individuals and legal entities, or entities subject to the sanctions addressed by Law No. 13,810 of 2019.
- Enable periodic training programs to ensure that all employees and independent agents are duly informed and up to date regarding their obligations and responsibilities in accordance with the applicable regulation;

RISK DEPARTMENT

- Identify, assess and monitor operational risk, liquidity risk and market risk, and report to Compliance if any atypical situation is identified; and

DISTRIBUTION DEPARTMENT

- Follow best practices regarding the “Know Your Client” process, especially in fundraising and intermediation, and also report suspicious activities to Compliance;
- Comply with internal procedures for identifying and maintaining the client registration records;
- Define procedures for identifying and obtaining registration data aimed at client identification and knowledge, as well as ensuring regulatory compliance;
- Define controls for validating the registration data declared by clients;
- Ensure that the client’s registration is in compliance with their status with the Brazilian Federal Revenue Service;
- Correctly and promptly fill out the Registration Form;
- Update the registration record within a period not exceeding that required by the regulation;
- Consult Compliance whenever there is an indication of irregularity or doubt as to the procedure to be adopted for the proper handling of the matter; and
- Identify Politically Exposed Persons, clients on restrictive lists, clients residing in border regions or holding nationality in a country considered sensitive for AML/CFT purposes, or those with a risk profession or risk activities, who follow a specific procedure, with the process only being carried out after the explicit authorization of the Compliance area;
- Annually, the registration area must carry out a validation test of the registration data of active clients.
- Report to Compliance if any Conflict of Interest is identified, in order to ensure that the trader performs their duties independently;
- Monitor atypical transactions;

- Observe the correct classification of transactions;
- Maintain transaction dossiers based on documents proving their legality;
- Assess whether transactions are in accordance with the operational modality and the client's technical qualification.

4.6 INFORMATION TECHNOLOGY DEPARTMENT

i. Ensure that the AML/CFT systems are functioning properly, ensuring the resolution of any failures in the shortest possible response time.

5. PROCESS FOR THE IDENTIFICATION AND HANDLING OF INDICATIONS OF MONEY LAUNDERING AND TERRORIST FINANCING

5.1. IDENTIFICATION

"Know Your Client" Client Identification Process, or KYC. This is a set of actions that establish mechanisms to ensure the identification, economic activity, origin and constitution of clients' assets and financial resources, including the capture, updating and storage of registration information, and also including specific procedures for identifying final beneficiaries and Politically Exposed Persons. Alaska does not permit the opening and maintenance of anonymous accounts. It is prohibited to initiate or maintain a relationship with individuals or entities mentioned in the financial sanctions lists of the United Nations (UN), the US Office of Foreign Assets Control (OFAC) and the European Union. Alaska adopts, as its main means of client registration, the electronic client identification form. The Distribution area is responsible for the analysis and recording of the information and identification documents of clients with whom the institution maintains a relationship. In order to improve the "Know Your Client" process, in addition to research on restrictive lists, Alaska carries out complementary research activities in relation to the client, such as: requesting additional documentation for clients in risk situations, and adopts specific internal procedures. Research on restrictive lists constitutes a preventive procedure that seeks to flag whether the client has been involved in money-laundering and terrorist-financing situations. These routines are intended to identify whether clients are politically exposed persons (PEP), whether they appear on any external restrictive list, hold a risk profession (internal list), and whether they reside in a border city. With regard to improving all practices related to the process of Anti-Money Laundering and Counter-Terrorist Financing related to cybercrimes, control is carried out through intelligent software that validates the data provided by the client, performing analysis of possible document fraud. When a client has a higher risk level, more detailed due diligence is carried out in the monitoring processes. Due diligence is carried out so that the institution identifies its clients and verifies information relevant to conducting business and transactions, mitigating the risks of financial crimes relevant to digital means. As a rule, all registrations must be updated within 24 (twenty-four) months from the last update, and this interval may be shorter depending on the Risk-Based Approach that Compliance adopts in relation to a given client. The risk-based approach process must take into account the following criteria: i - business relationships involving PEPs or non-profit organizations; ii - business relationships with clients and/or final beneficiaries or third parties domiciled in a high-risk country, as classified by FATF; iii - financial institutions operating with offshore products; iv - clients operating in businesses classified as high risk in the institution's RBA; v – activities with indications of atypicality of which it is aware; vi - reports of transactions that have been considered atypical of which it becomes aware; vii - inquiries from government authorities, such as subpoenas relating to ML/TF offenses; viii - transactions that violate economic sanctions programs; and ix - transactions with significant volumes and amounts incompatible with the client's source of income or inconsistent with those historically carried out. Client identification must contain, at a minimum, all the information set out in Annex B of CVM Resolution No. 50 of August 31, 2021, with the Compliance Officer being responsible for deciding whether to require additional documents based on their risk-based approach.

"Know Your Supplier" Process

This is a set of rules and procedures that must be adopted for the identification and acceptance of suppliers and service providers, preventing the engagement of untrustworthy companies or those suspected of involvement in illicit activities. For those representing greater risk, complementary procedures and in-depth assessment due diligence and specific approval levels must be adopted, according to the severity of the findings or exceptions. "Know Your Partner" Process. This is a set of rules, procedures and controls that must be adopted for the identification and acceptance of business partners, aiming to prevent doing business with untrustworthy counterparties or those suspected of involvement in illicit activities, as well as ensuring that they have adequate AML/CFT procedures, where applicable.

"Know Your Employee" Process

The first stage when hiring an employee consists of resume screening, in which the needs of the desired position and the suitability of the candidate's profile are analyzed, and the candidate is then invited to take tests that assess logical and mathematical abilities and technological knowledge. Approved candidates proceed to in-person interviews with Alaska's partners and employees. If the candidate is approved in all the previous stages, the Compliance Officer researches the candidate on restrictive lists and judicial convictions, and analyzes whether the documents sent by the candidate match the research carried out, which may include research with previous employers. Research on restrictive lists and judicial convictions constitutes a preventive procedure that seeks to flag the candidate's integrity and check for any inconsistency in the candidate's profile for the position of Alaska employee. The economic-financial situation is also analyzed, aiming to avoid ties with people involved in unlawful acts or with financial problems that could cause problems for Alaska. Alaska only hires candidates who attest to their integrity, and does not hire employees with criminal convictions, including but not limited to crimes of corruption, money laundering and terrorist financing, or crimes against the capital markets in general.

Assessment of New Products and Services

The Compliance area advises the Executive Committee to assess, in advance, from an AML/CFT perspective, new products and services, with the aim of mitigating regulatory risks and the risks of such products being involved in and/or used for the practice of money laundering or terrorist financing crimes.

Gifts and Giveaways Policy

All gifts or giveaways received by any Alaska employee, partner or officer as a result of performing their duties at Alaska must be reported to the Compliance Officer, who must assess the relevance and whether the gift could constitute a conflict of interest or otherwise interfere with Alaska's good practices. Gifts and giveaways not exceeding R$ 500.00 (five hundred reais) are excluded.

5.1.2 TRANSACTION MONITORING

The Compliance department is responsible for the transaction-monitoring routines for identifying indications of Money Laundering and Terrorist Financing. Monitoring is carried out through processes that collect clients' registration and operational information and financial transactions, through rule parameterization. Once an occurrence is generated, it is Compliance's responsibility to analyze the client and their transactions to confirm or rule out the indications of Money Laundering and Terrorist Financing. As a result of any identification of indications of Money Laundering, corruption or Terrorist Financing on the part of clients, Alaska may resolve to block the client's account and/or terminate the relationship.

5.1.3 REPORTING OF SUSPICIOUS TRANSACTIONS TO REGULATORY BODIES

Transactions, situations or proposals with indications of money laundering or terrorist financing must be reported to the competent regulatory bodies, when applicable, in compliance with legal and regulatory requirements. Good-faith reports do not give rise to civil or administrative liability for Alaska, its officers and employees. Information about the reports is restricted and not disclosed to clients or third parties. Reports must be made by the Compliance Officer to COAF, or the government body that replaces it, within 24 (twenty-four) hours, under the terms of the law.

5.2 BLOCKING OR TERMINATION OF THE RELATIONSHIP

As a result of any identification of indications of Money Laundering, corruption or Terrorist Financing on the part of clients, Alaska may resolve to block the client's account or terminate the relationship, as well as possibly report to the regulatory bodies, in accordance with the resolution of the Executive Committee.

6. MAINTENANCE OF INFORMATION AND RECORDS

Documents relating to transactions, including recordings and registration documents, must be archived for a minimum period of 10 (ten) years from the closing of the account or the completion of the client's last transaction.

7. CONFIDENTIALITY OF INFORMATION

All information related to data on indications/suspicions of money laundering and counter-terrorist financing is confidential in nature and must under no circumstances be made available to the parties involved, and must only be reported to the competent authorities. Should any employee report to the Compliance Officer, or should the Compliance Officer identify any indication of a violation, the

Compliance Officer must investigate confidentially, and may use external consultants or report to the competent public administration body so as not to compromise the investigations.

8. EXCEPTIONS AND APPLICABLE SANCTIONS

For cases of exception to compliance with the rules set out in this Policy, the requester must submit an exception request to the Executive Board with the reasons supporting it, and approval of the request must be given by at least two officers to whom the Policy applies.

Applicable Sanctions

Failure to comply with the legal and regulatory provisions subjects employees and partners to sanctions ranging from administrative to criminal penalties, for Money Laundering, Terrorist Financing and Fraud. Negligence and voluntary failure are considered non-compliance with this Policy and the Code of Ethics and Conduct, and are subject to the application of disciplinary measures provided for in internal regulations.

9. ANTI-CORRUPTION. Principles and definitions:

Combating corruption is a fundamental duty of Alaska and all of its Employees. The Anti-Corruption Rules establish that individuals and legal entities will be held strictly liable, in the administrative and civil spheres, for harmful acts committed by their partners and Employees against the public administration, whether national or foreign, without prejudice to the individual liability of the perpetrator, co-perpetrator or accomplice in the unlawful act, to the extent of their culpability. All employees must cooperate and assist in any investigation involving public officials, whether an internal investigation or one conducted by government oversight bodies. A "public official", and therefore subject to the Anti-Corruption Rules, is considered to include, without limitation:

(i) any individual who, even temporarily and without compensation, is in the service of, employed by, or holding a public function in a governmental entity, a government-controlled entity, or a government-owned entity, whether national or international;

(ii) any individual who is a candidate for, or holds, a public office, whether national or international; and

(iii) any political party or representative of a political party, whether national or international. Foreign public administration is considered to include state bodies and entities or diplomatic representations of a foreign country, of any level or sphere of government, as well as legal entities directly or indirectly controlled by the public authorities of a foreign country and international public organizations. The same requirements and restrictions also apply to family members of public officials up to the second degree (spouses, children and stepchildren, parents, grandparents, siblings, uncles/aunts and nephews/nieces) and close associates (individuals known to have joint ownership or partnership in companies or in arrangements without legal personality, who act as proxies, even under a private instrument, or who have any other type of close, publicly known relationship with the public official). Representatives of public pension funds, notaries and advisors to public officials must also be considered "public officials" for the purposes of this Policy. Alaska extends this definition to all those considered Politically Exposed Persons (PEPs). All meetings with persons covered by the definitions above must be attended by at least 2 Alaska employees, one of whom must be the Compliance Officer. Any financial transaction with public officials or persons covered by the definitions above must have accounting records that are accurate, complete, true and validated by an external accounting firm. It is strictly prohibited to:

(a) Promise, offer or give, directly or indirectly, an improper advantage, whether economic or not, to a public official, or to a third party related to them;

(b) Finance, fund, sponsor or in any way subsidize the practice of the unlawful acts provided for in the Anti-Corruption Rules;

(c) Use an intermediary individual or legal entity to hide or disguise their real interests or the identity of the beneficiaries of the acts performed;

(d) With regard to public bids and contracts: (i) thwart or defraud, through agreement, collusion or any other means, the competitive nature of a public bidding procedure; (ii) prevent, disrupt or defraud the carrying out of any act of a public bidding procedure;

(iii) remove or seek to remove a bidder, through fraud or the offer of any type of advantage; (iv) defraud a public bid or a contract arising from it; (v) fraudulently or irregularly create a legal entity to participate in a public bid or enter into an administrative contract; (vi) fraudulently obtain an improper advantage or benefit from modifications or extensions of contracts entered into with the public administration, without authorization in law, in the public bid notice or in the respective contractual instruments; or (vii) manipulate or defraud the economic-financial balance of contracts entered into with the public administration; (viii) hinder the investigative or oversight activity of public bodies, entities or officials, or interfere in their actions, including within regulatory agencies and national-financial-system oversight bodies; and (ix) give or offer any amount, hospitality (travel, meals, lodging and entertainment), giveaway or gift to a public official without the prior authorization of the Compliance Officer.

10. TRAINING

Compliance provides all employees and partners with training aimed at reviewing the concepts contained in this Policy and encouraging the adoption of appropriate measures in cases of suspected Corruption, Money Laundering and Terrorist Financing, or irregularities in the KYP and KYC processes. Annually, Compliance reviews the materials and everyone is required to undergo new training.