ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM FINANCING POLICY

REVISION CONTROL

REV.	DATE	DESCRIPTION	PREPARED BY	REVIEWED BY	APPROVED BY
00	15/07/2024	Initial Issue	Mariana Braga	Marcelo Monteiro	João Araújo
01	20/02/2025	Document Revision	Mariana Braga	Marcelo Monteiro	João Araújo

1 OBJECTIVE

This Policy aims to establish guidelines, responsibilities, and procedures designed to combat and prevent money laundering and the financing of terrorism in operations related to registration, financial transactions, contract management, and benefits administration.

It also seeks to guide and establish mechanisms that promote compliance with and adherence to operational procedures by all employees, directors, board members, participants, and third parties of **INNOVA GLOBAL BUSINESS**.

INNOVA GLOBAL BUSINESS condemns and does not tolerate any practices involving corruption, extortion, bribery, theft, kickbacks, fraud, money laundering, financing of terrorism, or any other unlawful acts. The limits set forth in this Policy are complementary to **Law No. 9.613, dated March 3, 1998**.

2 REFERENCE DOCUMENTS

Code of Ethical Conduct of Innova Global Business
Law No. 9.613/1998 (Money Laundering Law)
Law No. 12.846/2013 (Anti-Corruption Law)
Federal Decree No. 11.129/2022

3 APPLICATION

This procedure applies to all operations related to registration, financial transactions, contract management, and benefits administration carried out by employees, directors, board members, and business partners (when they do not have a similar policy) at any hierarchical level of **INNOVA GLOBAL BUSINESS**.

4 DEFINITIONS AND ACRONYMS

Money Laundering: a criminal offense aimed at converting illicit assets into legitimate ones, in order to conceal the true source, movement, location, origin, consistency, and ownership of assets and rights derived from criminal activities, whether directly or indirectly.
Third Parties: service providers, suppliers, sponsors, business partners, representatives, among others.
Financing of Terrorism: the gathering of funds and/or capital for the execution of terrorist activities.

Concealment: the stage that involves making it difficult to trace the accounting trail of illicit resources. Criminals, through electronic transactions, transfer funds to fictitious accounts or invest in financial instruments with the intent of breaking the chain of evidence.

5 GUIDELINES

The **INNOVA GLOBAL BUSINESS**:

5.1 Rejects any practices involving money laundering, terrorist financing, financing the proliferation of weapons of mass destruction, corruption, or any other unlawful acts.

5.2 Maintains senior management committed to the effectiveness and continuous improvement of this Policy, its procedures, and internal controls related to the prevention of money laundering and terrorist financing, and periodically submits relevant reports to the Executive Board for review.

5.3 Implements a governance structure dedicated to complying with this Policy and the obligations of preventing money laundering and terrorist financing, as defined by Law No. 9.613/1998.

5.4 Establishes procedures for internal risk assessment aimed at identifying and measuring the risk of its products, services, and business relationships being used for money laundering or terrorist financing. This assessment considers customer risk profiles; institutional risk (including business model and geographic scope); the nature of operations, transactions, products, and services (including distribution channels and new technologies); and the activities of employees, partner institutions, and suppliers.

5.5 Adopts procedures for assessing risks in the development of new products and services, as well as in the use of new technologies, to prevent money laundering and terrorist financing.

5.6 Conducts an annual evaluation of compliance and effectiveness of this Policy, procedures, and internal controls concerning money laundering and terrorist financing prevention, to identify potential deficiencies.

5.7 Issues an annual report containing the results of the control effectiveness evaluation referred to in item 1.6 of this Policy and submits it to the Executive Board for review.

5.8 Implements action plans to mitigate risks and correct deficiencies identified in inspections by regulatory authorities or in assessments conducted by Internal Controls and Internal Audit, specifically regarding anti–money laundering and counter–terrorist financing (AML/CTF) procedures.

5.9 Promotes an organizational culture of AML/CTF awareness through continuous training programs and targeted communications.

5.10 Provides annual training for employees on the prevention and combat of money laundering and terrorist financing, according to the company’s training matrix.

5.11 Applies due diligence procedures—Know Your Customer (KYC), Know Your Supplier (KYS), Know Your Partner (KYP), and Know Your Employee (KYE)—to mitigate AML/CTF risks according to the nature of activities, jurisdiction, and involved parties. These procedures include collecting, verifying, validating, and updating registration information, as defined in internal procedures.

5.12 Enforces restrictive measures on conducting business or maintaining relationships with customers, suppliers, partners, and employees whenever there is evidence of involvement in money laundering, terrorist financing, financing of weapons of mass destruction, corruption, or any other illicit activities, in compliance with applicable law.

5.13 Establishes procedures for identifying and approving relationships with customers, partners, service providers, and employees who may be classified as Politically Exposed Persons (PEPs) or related individuals, ensuring appropriate governance as defined in internal regulations.

5.14 Pays special attention to operations or proposed transactions involving PEPs, whether directly or through representatives, family members, or close associates.

5.15 Implements controls to ensure that all transaction settlements and fund movements occur exclusively through accounts (checking, savings, prepaid cards, or payment accounts) owned by verified customers affiliated with the company.

5.16 Utilizes internal systems for recording and monitoring transactions, configured to identify potential indicators of money laundering, terrorist financing, financing of weapons of mass destruction, corruption, and other illicit activities.

5.17 In transaction analysis, evaluates payment methods, frequency, involved parties, transaction values, patterns, economic activity, and any other indicators of irregularity or illegality, to detect potential signs of money laundering, terrorist financing, or corruption.

5.18 Maintains specific channels for receiving reports or complaints, including anonymous submissions, and strictly prohibits any acts of retaliation against whistleblowers acting in good faith.

5.19 Investigates signs and reports of suspected money laundering or terrorist financing activities conducted by employees or third parties against the company’s assets, in accordance with applicable laws.

5.20 Reports to competent authorities any transactions or proposed transactions that, under applicable law, present indicators of money laundering, terrorist financing, financing of weapons of mass destruction, or corruption.

5.21 Cooperates with public authorities in investigations related to money laundering, terrorist financing, proliferation financing, or corruption arising from its activities, in compliance with current legislation.

5.22 Conducts, confidentially, all processes related to the registration, analysis, and reporting of transactions with AML/CTF indicators to competent authorities.

5.23 Requires that any suspicious fact or evidence of direct or indirect involvement in criminal activity—whether or not covered by previous items—must be reported to the Compliance and AML departments.

5.24 Is committed to the continuous improvement of monitoring, screening, analysis, and reporting activities by regularly reviewing and updating its processes with a focus on intelligence and technology.

5.25 Reviews the guidelines established in this Policy annually and/or whenever there are process changes that may impact or justify its revision.

6 Stages of Money Laundering

There are three basic stages that make up the money laundering process, which must be properly understood by all interested parties in order to prevent and repudiate such criminal practices as much as possible. The stages of the crime of money laundering are:

6.1 Placement: This stage consists of the removal of financial amounts obtained through illicit activities and their introduction into the economic system. This phase is characterized by financial transactions and contractual agreements involving assets derived from criminal practices.

6.2 Layering (Concealment): This stage involves the manipulation of illicit resources already introduced into the economic system in order to achieve dispersion or eliminate traces of irregularities. It can be characterized by complex financial transactions and the simulation of business relationships, all aimed at disguising the illicit origin of the funds handled.

6.3 Integration: At this stage, the funds acquire a lawful appearance and become part of the financial system, making the illicit origin of the monetary amounts apparently unrecognizable.

7 PREVENTIVE PRACTICES AND INTENTIONAL PRACTICES

7.1 Preventive Practices – These are practices that can be adopted with the objective of preventing the occurrence of money laundering activities:

• Properly record and document information related to accounting transactions;

• Avoid carrying out economic, financial, or equity operations outside the commercial and tax books;

• Avoid, as much as possible, making payments in cash or through bearer instruments, except in cases expressly authorized by Senior Management;

• Broadly avoid making or receiving payments in bank accounts outside Brazil, except when the recipient is proven to be based abroad;

• Never make payments to foreign accounts without identifying the recipient;
• Avoid, as much as possible, transactions with countries considered “tax havens” under Brazilian legislation (IN RFB No. 1037/2010);
• Never make payments to individual bank accounts when the contract lists a legal entity as the contracting or contracted party;
• Make payments only to the account held by the contracted party, who must have demonstrably provided the service or supplied the good stipulated in the agreement;
• Avoid, as much as possible, making advance payments prior to the signing of a contract.

7.2 Intentional Practices – **These are indicators that may demonstrate the possible occurrence of money laundering:**

• Payments made in cash rather than through bank account deposits;
• Payments made to someone other than the rightful creditor, or to multiple beneficiaries;
• Payments made abroad without proven connection to the signed contract;
• Payments made without specifying the service rendered in return;
• Payments made unjustifiably in advance;
• Payments made in exchange for services without a contractual instrument;
• Resistance or refusal to provide requested information about a financial transaction.• Financial transactions involving amounts that are incompatible with the scope of the contract.

8 RESPONSIBILITY AND AUTHORITY

Management: Comply with and enforce this policy; oversee and monitor financial transactions; and report any suspected cases of money laundering or terrorist financing.

Compliance Function: The Compliance function is responsible for monitoring and reporting occurrences of financial transactions classified as suspicious under the legislation for the prevention of money laundering and terrorist financing.

Finance Department: Carry out payments and financial controls in accordance with this policy and procedure INN PRO FIN 001 – Financial Controls.

Other Employees and Interested Parties: All employees and interested parties are responsible for reporting any financial transactions that show signs of money laundering or terrorist financing activities.