ANTI-MONEY LAUNDERING AND COUNTER TERRORISM FINANCING POLICY
PETRO RIO S.A.

TABLE OF CONTENTS

1. Introduction

1.1 Purpose

The purpose of this Policy is to reinforce PetroRio's commitment to comply with national and international laws and regulations relating to Money Laundering and Terrorism Financing crimes and to instruct its employees and third parties acting on its behalf or in its favor the correct identification of the crime, in order to safeguard the values of PetroRio, its image, interests of the shareholders and other related parties.

1.2 Scope

This Policy applies to all councilors, directors, employees, third parties, and all persons working directly or indirectly for PetroRio, its subsidiaries, jointly controlled companies, joint ventures, business and commercial partners with whom PetroRio has business relationship, regardless of the nature of the relationship, whether continuous or occasional, whether it involves the transfer of financial resources or only knowledge (know-how).

Any employee and/or third party acting on behalf of or for the benefit of PetroRio must know and comply with this Policy, other related and applicable laws, and report possible violations to direct supervisor, contract manager, Compliance Department or report concerns on the Integrity Channel, whose access is available on PetroRio's website and its intranet.

2. Concept and Definitions

2.1 Money Laundering

The purpose of the Money Laundering crime is to conceal or hide the illicit origin of certain financial or other assets , so that such assets appear to be lawful, or at least illicit origin is difficult to prove.

The crime of money laundering has three stages:

Placement: In this stage, the criminal puts the dirty money in the market, usually in the form of a bank deposit in cash, in a financial institution with legitimate action. The deposit of large amounts of money is atypical and is considered as evidence of money laundering, leading banks to inform the competent financial intelligence bodies (e.g.: COAF - Financial Activities Control Council in Brazil; CSSF - Commission de Surveillance du Secteur Financier in Luxembourg) on the transaction. In this way, criminals often make several deposits with small amounts of money, an operation called “structuring”. The placement also occurs through the purchase of tradable assets (shares on a stock exchange) or the purchase of assets (e.g.: jewelry, vehicles, work of art, precious stones, etc.).

Layering: it is the camouflaging/"purification" of dirty money by spraying it through various financial transactions in order to break the chain of evidence and hinder its tracking. Layering can be done via wire transfers to anonymous accounts, especially in countries covered by banking secrecy law or considered tax havens, making deposits and withdrawals to change account balances, currency exchange and purchase of expensive items for the purpose of changing the "money type", by making deposits in accounts opened in names of "straw-mans" or using fictitious or front companies. The objective is to make it difficult to identify the origin of the resource.

Integration: it is the dirty money reintroduced into the economic system in a legitimate way. It occurs, for example, through investment in lawful business in the various sectors of the economy.

2.2 Terrorism Financing

The terrorist financing crime is classified by any financial support provided to the activities of terrorist individuals or groups or to an act constituting an offense under the terms of the applicable law.

Terrorism consists in the practice by one or more individuals of the acts provided for by law, for reasons of xenophobia, discrimination or prejudice of race, color, ethnicity and religion, when committed with the purpose of provoking social or widespread terror, jeopardizing people, properties, public peace or public safety.

2.3 Complementary Definitions

For purposes of this Policy, some terms must be understood as follows:

Employees: Any natural person who has a statutory/fiduciary relationship with the Company or who provides non-contingent (routinely) and onerous (receiving a salary) services to PetroRio, and is subordinate to the company, acting under its guidance. It includes, in addition to the employee hired under the Brazilian Labor Consolidation Law (CLT), Luxembourg Labor Law or other correspondent, interns, minor apprentices and temporary employees.

Fictitious company: A legally constituted company that carries out legitimate trade/activities, but which is used to account for resources from illicit activities. There is, in most cases, a mix of illicit resources with resources coming from their own activity.

Front company: Company established only in documents (only on paper, with no economic activity) in order to account for resources derived from the crime.

Structuring: Fractionation of the money originating from the crime in amounts lower than the limit established by the regulatory bodies for the communication of the operation.

Fraudulent Exports - Overbilling: Consists of the issuance of export invoices with a higher value than the transaction, the difference being paid with values of illicit origin. The distorted export operation covers the resources of criminal origin, making it possible to receive resources from abroad (resources to be "laundered", or integration of resources already "laundered").

Fraudulent Imports - Overbilling: Consists of the issuance of import invoices with a higher value than the transaction, the difference being paid with values of illicit origin. The distorted import operation covers the resources of criminal origin, making it possible to send illicit resources abroad, as payment for imported products.

Straw-man: Uncertain origin word regularly used to refer to someone who carries out commercial and financial transactions on their behalf, by order of third party, hiding the identity of the real agent or beneficiary; or who "lends" the name, and in some cases is also remunerated for the "provision of services", to hide the origin or the recipient of illicit money, especially in operations related to money laundering, corruption and financing of terrorism. There are situations in which innocent people, most of the time with limited education and low purchasing power, are used as "straw-mans", or in which documents lost or stolen are used by criminals to create "straw-mans". Also known as "figurehead".

Legitimate: Established and protected by law.

Lawful: That which is permitted by law, according to the law.

Tax Haven(s): Territories in which there is no State intervention in the economic activity at tax level, allowing the activities and transactions of a commercial and financial nature, provided that they are international, to be conducted without originating them the obligation to pay any taxes[1]. In practice, what makes certain localities "tax havens" is the conjunction of a fiscally moderate State (ie, which has no high taxation), with business protection, via fiscal, bank, and mainly corporate secrecy, and other different "conveniences". Some countries' financial control bodies list the countries or agencies with favored taxation and privileged tax regimes.

Politically Exposed Person (PEP): Persons considered politically exposed are: (i) the holders of elective mandates of the Executive and Legislative Branches of the Union; (ii) the occupants of the Executive Branch of the Union, Minister of State or equivalent, special nature or equivalent, president, vice president and director, or equivalent, of entities of the indirect public administration and the Direction and Superior Advisory Group - DAS , level 6, or equivalent; (iii) members of the Federal Supreme Court, Superior Courts and Regional Federal, Labor and Electoral Courts; (iv) the Attorney General of the Republic, the Attorney General of Labor, the Attorney General of the Military Justice and the Attorneys General of the States and the Federal District Justice; (v) the members of the Court of Auditors of the Union and the Public Prosecutor at the Court of Auditors of the Union; (vi) national presidents and treasurers, or equivalent, of political parties; (vii) the governors and secretaries of State and of the Federal District, the State and District Deputies, the presidents, or equivalent, of entities of state and district indirect public administration and the presidents of Courts of Justice, Military, Accounts or equivalent of the State and the Federal District; (viii) Mayors, Councilors, Presidents of Courts of Accounts or equivalent of Municipalities. Also considered politically exposed are those who, abroad, are: (i) heads of state or government; (ii) senior politicians; (iii) occupants of higher-level government positions; (iv) general officers and senior members of the judiciary; (v) senior executives of public companies; (vi) leaders of political parties; (vii) Directors, Deputy Directors, Members of the International Board of Directors; and (viii) brothers and sisters of PEPs. (COAF Resolution No. 29 of 2017 and Law of November 12, 2014, as amended by the Law of February 13, 2018)

Third Parties: Any natural or legal person that acts directly or indirectly on behalf of or in favor of PetroRio, in the capacity of service provider, supplier, consultant, regardless of formal contract.

[1] SILVA, Ruben Fonseca e; WILLIAMS, Robert E. **Tratados dos Paraísos Fiscais**. São Paulo: Observador Legal, 1998, p. 20.

3. Relevant Rules and Legislation

Numerous are the laws and regulations that deal with money laundering and terrorism financing. The following are the main ones to be observed:

- **Law no. 9.613/98:** Provides for crimes of "laundering" or concealment of assets, rights and values; the prevention of the use of the financial system for the respective crimes and creates the COAF - Financial Activities Control Council;
- **CVM Instruction no. 301/99, as amended by CVM Instruction 463/08:** Provides for the identification, registration, operations, communication, limits and administrative responsibility related to crimes of laundering or concealment of property, rights and values - the provisions of this instruction must be observed to refer to PetroRio's activities;
- **Circular Letter no. 3.542/12 of the Central Bank of Brazil "BACEN":** Discloses a list of operations and situations that may establish indications of the occurrence of the crimes provided for in Law No. 9.613, dated March 3, 1998, which may be communicated to COAF- Financial Activities Control Council - the provisions of this instruction must be observed to reference the activities of PetroRio;
- **BACEN Circular no. 3461/09:** Provides for procedures to be adopted to prevent and combat activities related to crimes under Law No. 9.613/98 - the provisions of this instruction must be observed to refer to PetroRio's activities;
- **BACEN Circular Letter no. 3430/10:** Clarifies aspects related to the prevention and combat of activities related to the crimes provided for in Law No. 9.613, of March 3, 1998, addressed in Circular No. 3.461, of July 24, 2009 - the provisions of this instruction must be observed to refer to PetroRio's activities;
- **Normative Instruction RFB no. 1037/10:** Relates countries or dependencies with favored taxation and privileged tax regimes;
- **Standards issued by COAF:** Financial Activities Control Council (http://fazenda.gov.br/orgaos/coaf/legislacao-e-normas/normas-2013-coaf);
- **Law of November 12, 2004:** Provides for the fight against Money Laundering and Terrorism Financing - the provisions of this law must be observed to refer to PetroRio's activities in Luxembourg;
- **Law of October 27, 2010:** Provides for prohibitions and restrictive financial measures against certain persons, entities and groups in the fight against the financing of terrorism - the provisions of this law must be observed to refer to the activities of PetroRio in Luxembourg;
- **Law of February 13, 2018:** introduces amendments, among others, in the Luxembourg law of November 12, 2004 on combating Money Laundering and Terrorism Financing - the provisions of this law should be observed to refer to the activities of PetroRio in Luxembourg.

The list of regulations above is exemplary, and others may be applied to PetroRio's or the Company's business used to refer to its activities, raising its governance level, and all employees and third parties acting on behalf of or in favor of PetroRio remain updated to new laws, editions or revocations.

4. Registration of Customers, Employees, Suppliers and Business Partners

The registration of customers, employees, suppliers and business partners is a primary and indispensable element in the fight against and prevention of money laundering crime, and compliance with the following rules is mandatory:

Obtaining and analyzing the minimum registration data of:

Legal Entities: Corporate Name, trading name, validity of the National Register of Legal Entities, Social Contract or Statute, registered in Notary Office or Commercial Registry, with the number of NIRE, CNAE according to the nature of the activity to be contracted, physical (tax and commercial) and electronic address, vertical (shareholders and invested companies) and horizontal (joint-venture, SCP, etc.) corporate structure;

Individuals: Name, Social Security, address, participation in companies, employment or commercial relationship with other companies.

- Third party due diligence history, in accordance with PetroRio's Code of Ethics and Conduct, Third Party Evaluation and Monitoring Policy and other related matters;
- Updating of registration data periodically;
- Conduction of thorough analysis of transactions executed during employment, commercial and business relationships to ensure they are consistent with the Company's knowledge of the third party, its business and risk profile.

All information must be carefully analyzed for the registration acceptance purpose, to certify its completeness and truthfulness.

It is forbidden the initiation or maintenance of relationships with individuals or entities mentioned in the financial sanctions lists of the United Nations (UN), the United States Office of Foreign Assets Control (OFAC), European Union, or registered in the CEIS/CNEP Integrated Registration System or CEPIM

The on-site evaluation of the infrastructure of the business and commercial partner, in order to verify the existence of the declared activity, the non-accomplishment, parallel to the formal and legally allowed activity, of illegal activity is recommended.

Regarding employees, the evaluation and monitoring of the standard of living, the coherence between this and the benefits arising from previous employment or PetroRio, or recognized and legitimate business activity (when not conflicting with the employment relationship) or family's financial resources. Also, media monitoring, which includes social networks, in order to identify extremist behaviors aimed at, among other things, the propagation of ideologies and recruitment of followers, and any other indications of (propensity for) terrorist activity.

5. Examples of the Money Laundering and Terrorism Financing Crime

5.1 Examples of Money Laundering Crime

In view of the various laws and regulations relating to the crime of money laundering, it is essential that all employees are aware of the possible ways in which the crime is committed, here are some practical examples:

- Incompatibility of transactions with the individual's net worth;
- Overbilling of contracted services (e.g.: fraudulent imports and exports/overbilling);
- Unusual operations in relation to the company's day-to-day operations (e.g.: unusual partners and unusual operating volumes);
- Operations in which the final beneficiary cannot be identified;
- Funds from various sources, especially from regions far from the legal entity's business area or from tax havens, or from bank accounts that are different from the commercial/business partner, without economic and financial grounds;
- Request for payment for a different account than the one held by the supplier, in its favor (for example, with the justification of the assumption of debt), fragmentation of the payment in a way that is different from the commercial agreement/signed contract or the commercial practices traditionally accepted in the place of business, or for an account registered in a tax haven;
- Payment of large amounts in cash or fragmented;
- Negotiations in foreign currency that are not compatible with the nature of the transaction;
- Request for non-compliance or action to induce employees of the Company not to follow internal procedures;
- Usual payments to suppliers or beneficiaries that do not have a connection with the activity or branch of business of the Company;
- Payments or wire transfers to a supplier far from the Company's business area, without economic-financial grounds;
- Usual movement of financial resources from or to politically exposed persons or persons of close relationship, not justified by economic events;
- Granting of power of attorney to a person outside the business.

The above and other situations considered to be atypical raising the suspicion of the money laundering offense must be reported immediately to your superior, to the Compliance Department or to the Integrity Channel.

5.2 Examples of Evidence of Terrorist Activity

The following situations, when combined, reveal signs of possible terrorist plans in progress:

- Falsification of documents such as passport, Social Security, Identity Card, Driver's License, among others;
- Acquisition and handling of weapons, ammunition, accessories and equipment for restricted use and without proper authorization;
- Acquisition and unauthorized handling of biological, chemical, nuclear, radiological products of controlled use;

- Acquisition on a large scale of permitted products, but which may be used for the manufacture of explosives, such as acetone, hydrogen peroxide, sulfuric acid, ammonium nitrate, among others;
- Unauthorized possession of data such as images, videos, plans, sketches, maps, positioning of cameras and watchmen of some public or private large circulation facility;
- Link with terrorist or extremist organizations;
- Sending money to terrorist or extremist organizations;
- Transfers of large sums of money to countries where there is greater activity of terrorists or where there are areas of conflict;
- Attempts at unauthorized access to restricted areas of large public or private facilities;
- Extreme speeches, including in social networks, of hate and incitement to violence;
- Dissemination of threats, including in social networks, of terrorist attacks;
- Isolation, distrust and alienation of family, friends and co-workers because they consider that they behave in an "impure" way;
- Change in habits, including food and clothing, to meet patterns established by radical groups, because there is a risk of deviation from the "true path";
- Frequent visits to extremist websites and social networks.

Suspicion of individual or collective terrorist activity; by any unauthorized personnel and, when not related to PetroRio's activities in the Company's premises, its customers or business partners, explosives, toxic gases, poisons, biological, chemical, nuclear or other means able to cause damage or promote mass destruction; the use of the Company's messaging, network and internet systems for the collection of funds for the financing, promotion, constitution or integration of a terrorist organization, or access to extremist content and social websites and networks, inviting or inciting terrorism; the use of PetroRio technologies for undue cyber action aimed at sabotage of essential public services as well as oil exploration, refining and processing, among other activities, must be immediately communicated to the Compliance area or registered in the Integrity Channel.

6. Control and Monitoring

PetroRio performs due diligence with the scope of comparing the registration information provided by its clients, employees and business partners in order to ensure that there is no evidence of operations that constitute the occurrence of crimes under the money laundering and terrorism financing laws, and other related matters, applicable to the Company's business. The analysis process will take place periodically and take into account reputational aspects, history of financial transactions and payment model, restrictive lists, origin and destination of resources, among other issues relevant to the preservation of PetroRio, its shareholders and stakeholders.

7. Training

In order to provide better protection conditions for PetroRio, and with the purpose to mitigate reputational, financial, regulatory and legal risks, periodic training is conducted to guide and enable all employees regarding the good understanding and alignment to the Money Laundering and Terrorism Financing prevention culture, as well as keeping everyone up-to-date on the relevant aspects pertinent to the subject.

8. General Conditions

8.1 Suspicion of Violation of Policy and Disciplinary Measures

All incidents or suspected breaches of this Policy will be treated, within reasonable limits, in a confidential manner, provided that the physical integrity or the life of employees of PetroRio and any third parties is not at risk, a situation in which the Company believes it to be its duty to inform immediately the competent authorities.

Failure to comply with the guidelines set forth herein and the related laws to which PetroRio is bound, including by omission, will result in the application of disciplinary measures or commercial sanctions to the perpetrator.

8.2 Reporting Concerns to the Integrity Channel

Any actual or potential breach of this Policy must be reported to the immediate superior, Compliance or reported on PetroRio's Integrity Channel, available on the Company's intranet and on its website.

The information registered in the Integrity Channel, or reported directly to the immediate superior or Compliance, will be treated as confidential, and the identity of the whistleblower will be preserved within reasonable limits, unless PetroRio is legally enforced to inform the government authorities.

8.3 No Retaliation

No retaliation will be tolerated against anyone who, in good faith, reports fact or suspicion of illegal conduct, breaches of this Policy, PetroRio’s Code of Ethics and Conduct, and other Company policies, or that cooperates in the investigation of possible frauds.

Retaliation, revenge, punishment, persecution or any form of constraint against the bona fide whistleblower and witnesses will result in the application of the sanctions provided for in PetroRio's Code of Ethics and Conduct or specific policy.

Annex A – Term of Acknowledgment

I hereby declare that I have received, read and understand the PetroRio Anti-Money Laundering and Counter Terrorism Financing Policy and I am aware of the established guidelines and their relevance to my activities with PetroRio.

I commit to comply fully with it and report its noncompliance, under penalty of being subject to the disciplinary measures set forth in PetroRio's Policy, Code of Ethics and Conduct, contract and current legislation.

_____(place), ____(day) of _____(month) of _____(year)

_____

Signature
Full Name:
ID: