

CHAPTER	04 - MONEY LAUNDERING PREVENTION AND TERRORISM FINANCING
SECTION	INSTITUTIONAL POLICY

OBJECTIVE

This policy sets forth the principles and guidelines of LASTTRO TRADING for the prevention of money laundering and terrorist financing practices ("PLDFT"), in line with current legislation and regulations and with good market practices, for the identification of operations and/or situations that present atypicality that may configure signs of Money Laundering and/or Financing of Terrorism.

For the purpose of this policy, crimes of "Laundering" or Concealment of Goods, Rights and Values are understood to be to hide or disguise the nature, origin, location, disposition, movement or ownership of goods, rights or values arising, directly or indirectly, out of criminal offence.

LASTTRO TRADING does not accept and will take the necessary measures against any form of transformation of funds originating from illegal activities into assets of apparently legal origin, customer knowledge, supported by training programs and the use of technological tools for monitoring financial transactions, aims to prevent the use of the company in transactions or situations that may be, directly or indirectly, linked to the crimes typified in Law 9.613/98.

These actions, combined with specific analyses, contribute to the full observance of the institutional policy, allowing the protection of LASTTRO TRADING, as well as its partners, administrators, employees, customers, partners and outsourced service providers.

MONEY LAUNDERING AND TERRORISM FINANCING PREVENTION ("PLDFT")

DEFINITION OF MONEY LAUNDERING

Money laundering is the criminal practice that consists of converting or transforming goods or money, obtained through illicit activities, into apparently lawful capital or even providing legal resources to be used for illicit purposes, by placing such goods or money in the Financial System.

MONEY LAUNDERING STEPS

The process (crime) aims to transform the illicitly generated resource, giving it a licit appearance, and can be divided into three stages:

- **PLACEMENT** is the process of introducing illegal resources into the National Financial System, usually through deposits or cash payments, without calling the attention of financial institutions, judicial authorities, or the government.

- **CONCEALMENT** is the process by which criminals try to drive illegal resources away from their origins by confusing and obscuring the clues by which the resources can be traced.

CHAPTER	04 - MONEY LAUNDERING PREVENTION AND TERRORISM FINANCING
SECTION	INSTITUTIONAL POLICY

Typically, concealment is characterized by carrying out a series of transactions involving different parties using wire transfers or other transfers of funds, often including “shell” companies or other bogus organizations, non-existent financial products, and different financial institutions.

- **INTEGRATION** is the last stage of the money laundering process and consists of criminal control over illegal resources in a way that appears to be legitimate. If successful, integration results in the reintroduction of illegal resources into the economy.

DEFINITION OF TERRORISM FINANCING

Terrorist financing is the process of raising awareness, concealing, or distributing resources to support or use terrorist activities or organizations.

Terrorist financing differs slightly from money laundering, in which, in general, terrorists use money that has been legally obtained or that has been laundered. Terrorists know that if they use illegally obtained money, there is a greater risk that they will be discovered before they can use it to finance their terrorist activities.

Money laundering and terrorist financing are two types of crime against the economic and financial order with devastating effects. In both cases, criminals or terrorists can exploit loopholes and weaknesses in a legitimate financial system to launder illegally obtained funds and support terrorist activities, unless necessary safeguards are put in place.

Operations related to terrorism, or its financing are those carried out by persons who carry out or plan to carry out terrorist acts, who participate in them or facilitate their commission, as well as by entities owned or controlled, directly or indirectly, by such persons or entities to act under his command.

REGULATORY ENVIRONMENT

- Federal Law no. 9.613 dated 03/03/1998 and later amendments;
- Federal Law no. 13.260 dated 03/16/2016;
- Federal Law no. 12.846 dated 08/01/2013;
- Federal Law no. 13.709 dated 08/14/2018;
- Resolution no. 23/2012 – by COAF (UIF);
- Resolution no. 29/2017 – by COAF (UIF);
- Normative Instruction No. 1571 – 07/02/2015 by (RFB);

CHAPTER	04 - MONEY LAUNDERING PREVENTION AND TERRORISM FINANCING
SECTION	INSTITUTIONAL POLICY

ROLES AND ACCOUNTABILITIES

RESPONSIBLE BOARD

- Approving LASTTRO TRADING's PLDFT guidelines and their respective reviews.

COMPLIANCE

- Managing the PLDFT program (complying and causing it to be complied with);
- Monitoring customer operations and the conduct of business channels;
- Coordinating PLDFT training with employees and partners;
- Reporting to the Risk and Compliance Committee cases considered atypical or suspicious detected in LASTTRO TRADING's business environment;
- Communicating to COAF (UIF) the operations or situations suspected of involvement with the crimes provided for in Law 9.613/98 upon resolution of the Compliance Risk Committee;
- Properly storing in physical and/or electronic media all documentation related to PLDFT activities for a minimum period of five years.
- Drafting an annual report containing the effectiveness of the PLDFT policy.

RISK AND COMPLIANCE COMMITTEE

- Ensuring together with the Compliance Area that the business channels are operating in accordance with LASTTRO TRADING's PLDFT policy;
- Previously assessing new products and/or services from a PLDFT perspective in order to identify inherent risks and establish preventive measures;
- Making decisions about communicating to COAF (UIF) of operations considered atypical and/or suspicious;
- Making decisions about disabling, temporarily or permanently, customers to carry out operations.

ENROLLMENT

- Validating customer registration information and keeping them up to date, under the terms of the regulations, or at any time, in case new relevant information emerges, paying special attention to those related to Politically Exposed Persons;
- Applying and evidencing procedures for verifying registration information proportionate to the risk of using products, services and distribution channels for money laundering and terrorist financing;
- Rating active customers by degree of risk, as provided for in the regulations.

INTERNAL AUDIT

- Assessing and testing the effectiveness of internal controls related to PLDFT;

CHAPTER	04 - MONEY LAUNDERING PREVENTION AND TERRORISM FINANCING
SECTION	INSTITUTIONAL POLICY

- Issuing analytical reports to Management and the Board, pointing out points of vulnerabilities and/or opportunities for improvement.

ALL EMPLOYEES AND COLLABORATORS

- Being familiarized with and complying with the guidelines of this policy;
- Timely meeting requests for documents and clarifications made by LASTTRO TRADING's Compliance Area;
- Reporting to the Compliance Area any and all operations, proposals for operations or atypical situations, as well as those that, due to their form, value or regularity, constitute an artifice that aims to circumvent LASTTRO TRADING's identification mechanisms, controls and records.

"PLDFT" PROGRAM

CUSTOMER RATING

In view of the operational characteristics of LASTTRO TRADING, every customer who trades in the precious metals market, in particular gold, MERCHANDISE, or FINANCIAL ASSETS, which is a common legal entity, jewelry store, mining company, financial institution and foreign customer will be considered as Customers.

INFORMATION REQUIRED FROM CUSTOMERS

Average monthly revenue amounts for the twelve months, and/or previous Balance Sheet, in the case of legal entities, the statement signed about the purposes and nature of the business relationship with LASTTRO TRADING.

POLITICALLY EXPOSED PERSON (PEP)

PEP is considered a public agent who performs or have performed, in the last five years, in Brazil or in foreign countries, territories and dependencies, positions, jobs or relevant public functions, as well as their representatives, family members and other people of their close relationship.

In the case of Brazilian customers, the following should be covered: holders of elective mandates of the executive and legislative branches of the federal government; the occupants of office, in the executive branch of the federal government; minister of state or equivalent; of a special or equivalent nature; president, vice-president and director, or equivalent, of indirect public administration entities; and the senior management and advisory group (das), level 6, or equivalent.

Members of the national justice council, the federal supreme court, the superior courts, the federal regional courts, the regional labor courts, the regional electoral courts, the superior labor justice council, and the federal justice council.

CHAPTER	04 - MONEY LAUNDERING PREVENTION AND TERRORISM FINANCING
SECTION	INSTITUTIONAL POLICY

Members of the national council of the public prosecutor's office, the Federal Prosecutor General, the Vice-Federal Prosecutor General, the Labor Prosecutor General, the Military Justice Prosecutor General, the Deputy Prosecutors General and the prosecutors general of justice from the States and the federal district, the members of the federal accounting court, the Prosecutor General and the Deputy Prosecutors General from the public prosecutor's office with the federal accounting court.

National presidents and treasurers, or equivalent, of political parties, state and federal district governors and secretaries, state and district deputies, presidents, or equivalent, of state and district indirect public administration entities and president's courts of justice, military courts, courts of accounts or equivalent of the states and the federal district.

Mayors, council members, municipal secretaries, presidents, or equivalent, of municipal indirect public administration entities and presidents of audit courts or equivalent of municipalities.

Also considered politically exposed are people who, abroad, are:

- Heads of State or Government; senior politicians; senior government officials, general officers, and senior members of the judiciary; senior executives of public companies, or leaders of political parties.

Politically exposed persons are also considered to be senior managers of entities governed by public or private international law.

In the case of customers residing abroad, the company must adopt at least two of the following measures:

- Requesting an express statement from the customer regarding their qualification;
- Making use of publicly available information;
- Referring to public or private databases on politically exposed persons.

The politically exposed person condition must be applied for the five years following the date on which the person ceased to perform.

Relatives, in the straight line, up to the second degree, the spouse, partner, companion, stepson and stepdaughter, and close collaborator are also considered PPE. For the beginning of the relationship, the Registration Area will characterize the customer as a PEP through consultation carried out in the list made available by the unit of the COAF Activities Control Council (UIF), as well as by the declaration signed by the customer himself.

Operations carried out with PEP will be subject to "enhanced monitoring and high risk".

CHAPTER	04 - MONEY LAUNDERING PREVENTION AND TERRORISM FINANCING
SECTION	INSTITUTIONAL POLICY

KNOW YOUR CUSTOMER (KYC)

It is a set of procedures and rules adopted to ensure the proper identification and end activity of customers, as well as the mineral origin and its traceability. In this way, LASTTRO TRADING will protect its reputation and reduce the risks of its products and services being used to legitimize resources from illegal activities.

OBJECTIVE (KYC)

The Know Your Customer (KYC) policy is one of the pillars that make up the PLDFT program and its objective is to inhibit the entry or retention of customers whose activities are linked to the crime of money laundering and/or financing of terrorism.

MISCELLANEOUS (KYC)

The concept of "Know Your Customer" is linked to the identification of the customer, which must be established before closing the deal. If he refuses or makes it difficult to provide the required registration information, LASTTRO TRADING will not accept him as a customer.

All LASTTRO TRADING employees must be diligent in preventing money laundering and combating the financing of terrorism, thus avoiding the occurrence of this illegal practice. They must also promptly report any atypical or suspicious transactions (or proposed transactions) to the Compliance Area.

The conquest or maintenance of a relationship with a customer must always be guided by the perspective of transparency and fairness of its activities, within the concept "Know your Customer", and not just by the commercial interest and/or profitability that this customer can provide in their relationship with LASTTRO TRADING.

GENERAL GUIDELINES (KYC)

CUSTOMER IDENTIFICATION AND VERIFICATION (KYC)

The identification process applies naturally at the beginning of the relationship. Identification is the act of confirming who a person claims to be by providing information. Verification, on the other hand, is the process of proving that a person is really who they claim to be through a thorough examination of the documents provided, that is to say, the documentary evidence must be satisfactory and dependable in identifying and registering the customer.

In the case of a legal entity, it is essential to know who owns the company and what the shareholding structure is until reaching the natural persons authorized to represent it, as well as the chain of shareholding until reaching the natural person characterized as the final beneficiary, i.e., one who exercises control or significant influence in management.

CHAPTER	04 - MONEY LAUNDERING PREVENTION AND TERRORISM FINANCING
SECTION	INSTITUTIONAL POLICY

CHECKING RESTRICTIVE LISTS (KYC)

Restrictive lists must be checked when entering the customer and in the respective registration updates. If it is found that the customer is on any impediment list or has been cited in any illicit event reported by the media, the Compliance Area must be notified in order to assess the initiation or maintenance of the relationship.

It is mandatory to check, at a minimum, the following sources:

- Financial Activities Control Council COAF (UIF): PEP-SISCOAF list;
- Internal Revenue Service: Validation of CNPJ;
- Office of Foreign Assets Control (OFAC): American Anti-Terrorism List.

PURPOSE OF THE BUSINESS RELATIONSHIP (KYC)

It is extremely important that a relationship be established with the customer, proactively, with the objective of knowing the real interest that led him to look for LASTTRO TRADING to carry out his operations.

COMPOSITION OF THE ELECTRONIC OR PHYSICAL DOSSIER (KYC)

The registration documentation required by LASTTRO TRADING must be stored electronically or physically, including evidence of consultations and searches carried out during the registration process.

KNOWING THE TRACEABILITY OF THE "GOLD" SUPPLY CHAIN (KYC)

The compatibility between the company's activity, its equity, its presumed financial capacity must be evaluated, as well as verifying the origin of the resources used and the traceability of the mineral origin.

Still in the case of mining companies, monitoring produced volumes, size and scale of their productive activities, and other indicators are in accordance with the origin of the metal, and with transactional volumes.

Among the measures adopted for the traceability of the gold supply chain, LASTTRO TRADING has the Precious Metals Origin Verification Policy, to ensure that the metals sold have a legal origin, as well as comply with Brazilian legislation, considering the environmental and human rights aspects.

CHAPTER	04 - MONEY LAUNDERING PREVENTION AND TERRORISM FINANCING
SECTION	INSTITUTIONAL POLICY

VISITING THE COMPANY'S FACILITIES (KYC)

The purpose of the visit is to understand the company's business and observe whether the mineral origin and volume transacted are consistent with the type, scale and size of the operation conducted by the company.

This is a practice of complementary analysis of company information, to measure and mitigate actual and potential risks, which are the responsibility of the director, employee, representative or agent who is prospecting the new customer, or negotiating with the current customer.

This rule DOES NOT APPLY to customers presenting medium and low risk, and foreign customers.

SURVEILLANCE (KYC)

The monitoring process is extremely important in the PLDFT program. Operations or situations that deviate from the expected standard must be reported to the Compliance department for proper treatment. This action is essential to subsidize the report to COAF (UIF).

Disappointing news and, mainly, related to financial crimes must be continuously monitored to mitigate the image risk.

RISK-BASED APPROACH (KYC)

Risk factors, drivers, or indicators (risk drivers) must be observed according to the conditions or characteristics that make a customer susceptible to being used to launder money, therefore, compliance analyzes will consider, among other aspects:

- Commercial segment and customer tradition;
- Nature of activity and how long it has been in the market;
- Customer geographic location (risk jurisdictions and border regions);
- PEP Customer;
- Source of funds (revenue and equity).

In this context, LASTTRO TRADING will adopt reinforced measures to mitigate such risks and where the risks are lower, simplified measures may be adopted, without prejudice to due diligence regarding customers.

Customers active in the Company will be classified by degree of risk:

LOW RISK:

Corporate Customers – (Banking Institution and Metal Refiners).

CHAPTER	04 - MONEY LAUNDERING PREVENTION AND TERRORISM FINANCING
SECTION	INSTITUTIONAL POLICY

MEAN RISK:

Corporate Customers – (Jewelry, Mining Companies and Foreign Customers with *more* than 12 months of activity).

HIGH RISK:

Corporate Customers – (Jewelry, Mining Companies and Foreign Customers with *less* than 12 months of activity).

Customers rated as HIGH RISK must prove bank reference and bank qualification.

All new products and services will be previously analyzed by the Compliance Committee in order to identify vulnerabilities from the perspective of preventing money laundering.

Any changes in registration information that are considered as aspects for classification in the Risk-Based Approach may change the customer's risk level.

PREPARATION AND UPDATE OF ENROLLMENT (KYC)

The registration documentation of customers considered active permanents must be renewed at intervals not exceeding 24 months, as for permanent customers who present a high risk, renewal will be at intervals not exceeding 12 months.

KNOW YOUR EMPLOYEE (KYE)

It is a set of procedures and regulations adopted for recruiting and monitoring employees in accordance with the precepts of PLDFT.

OBJECTIVE (KYE)

The Know Your Employee (KYE) policy was established based on ethical and behavioral values and aims to establish guidelines aimed at mitigating the risk of using LASTTRO TRADING in illegal practices of any nature, including, among them, money laundering, terrorist financing and corruption.

CRITERIA FOR RECRUITMENT (KYE)**SELECTION (KYE)**

Any need for hiring will be carefully analyzed to verify that there is no possibility of internal use of resources.

CHAPTER	04 - MONEY LAUNDERING PREVENTION AND TERRORISM FINANCING
SECTION	INSTITUTIONAL POLICY

Once this possibility has been exhausted, the requesting area will define the technical requirements and desired profile of the professional to be hired.

The candidate recruitment and selection process at LASTTRO TRADING will include verification of the candidate's professional history, as well as the existence of unflattering facts.

The approved candidate will be forwarded to the administrative area, for the following measures: (i) medical examination; (ii) obtaining the necessary documentation for hiring in accordance with CLT - Consolidated Labor Laws.

HIRING (KYE)

In possession of the medical examination and all the documentation requested by LASTTRO TRADING, the administrative area will properly formalize the contract with the respective professional.

If the contractor is a legal entity, LASTTRO TRADING will request a copy of the Articles of Incorporation.

The contracted professional will receive the "MCI - PLDFT" and will sign a "Term of Receipt" with LASTTRO TRADING in 2 (two) copies, the original of the Term will be kept in the employee's medical record and the 2nd copy with the employee, the whole process will be formalized via Minutes.

FOLLOW-UP (KYE)

If LASTTRO TRADING detects a sudden change in the economic pattern of its employees, prudential actions will be promoted that make it possible to identify possible illicit origins.

KNOW YOUR PARTNER (KYP)

It is a set of procedures and rules adopted to ensure the proper identification and good reputation of the future service provider for carrying out operations or services provided on behalf of LASTTRO TRADING, as well as control and surveillance mechanisms.

OBJECTIVE (KYP)

LASTTRO TRADING understands that commercial partnerships are important for its business model, however, it recognizes that it may represent a potential risk if not properly assessed and managed.

Based on good market practices, LASTTRO TRADING requires all its employees to properly identify the new Partner prior to starting the relationship and entering into an agreement.

CHAPTER	04 - MONEY LAUNDERING PREVENTION AND TERRORISM FINANCING
SECTION	INSTITUTIONAL POLICY

In this context, LASTTRO TRADING implemented the present procedure known as Know Your Partner (KYP), which applies to all service providers that enter into a Service Provision Agreement ("Agreement") to carry out operations in the gold and services provided to LASTTRO TRADING.

GENERAL GUIDELINES (KYP)

Initiate relationship only with Partners that comply with the applicable legal requirements; Maintain an open and honest dialogue with Partners, in accordance with good business practices; Protect any confidential information of LASTTRO TRADING either by its own nature or because of the agreement signed with the Partner.

PRIOR CHECKING (*DUE DILIGENCE*) (KYP)

At LASTTRO TRADING, the approval process for new Partners will be based on "due diligence" and relies on the coordinated action of the areas involved, as described below.

DOCUMENTATION (KYP)

The process is coordinated by the compliance area, which prepares a dossier containing the Partner's information and documents and all information and documents must comply with the prerogatives of LASTTRO TRADING, in addition, they must be obtained within the criterion of reasonableness and materiality.

APPROVAL (KYP)

LASTTRO TRADING's Risk and Compliance Committee will evaluate all aspects, especially the "reputational", using all control mechanisms and publicly available information.

Depending on the specific case, the Risk and Compliance Committee may request additional documents and/or information from the company for further assessment (focused on risk).

The approval or refusal will be formalized in the Minutes of the Meeting and must be duly filed by the Compliance area.

PRECLUSIONS (KYP)

LASTTRO TRADING shall not accept as partner:

- Companies potentially involved with negative images and possible criminal practices;
- Companies whose documentation and/or conduct do not allow identifying the legitimacy of their activities;
- Existence of facts, which at the discretion of LASTTRO TRADING, discredit the company and its owners.

CHAPTER	04 - MONEY LAUNDERING PREVENTION AND TERRORISM FINANCING
SECTION	INSTITUTIONAL POLICY

CRITERIA FOR PAYMENTS AND RECEIPTS

PURCHASE OPERATIONS

Purchase operations (gold or other precious metals) must be paid by LASTTRO TRADING through:

a) Available Electronic Transfer (TED) or any other bank transfer order for funds, including international SWIFT, issued to the seller and that the funds are credited to the deposit account held by him.

SALE OPERATIONS

Sales operations and exports may be received by LASTTRO TRADING through:

a) Available Electronic Transfer (TED) or any other bank transfer order for funds, including international SWIFT, international remittances, issued by the buyer and that the funds are debited from the deposit account held by him.

TRAINING

PLDFT training is mandatory for "all" LASTTRO TRADING employees, as well as everyone who is directly involved in the operation.

The training can be carried out in person or at a distance and in partnership with specialized companies or class entities, of recognized technical capacity and approved by LASTTRO TRADING.

All training must contain the topic dealing with "MONEY LAUNDERING PREVENTION AND TERRORISM FINANCING" and verification of good mineral origin, with a minimum workload of 2 hours, with mandatory renewal within a period of no more than 18 months.

At the end of the training, all employees and collaborators must carry out a final evaluation to receive the certificate of completion, whose minimum passing grade must be 70%.

MONITORING

The activities of continuous monitoring of operations aim to ensure that LASTTRO TRADING's businesses are being carried out in "compliance", with the established rules, continuously monitoring all operations and situations that may, after detection and respective analysis, constitute evidence of PLDFT.

CHAPTER	04 - MONEY LAUNDERING PREVENTION AND TERRORISM FINANCING
SECTION	INSTITUTIONAL POLICY

I - SITUATIONS ARISING FROM THE CUSTOMER IDENTIFICATION PROCESS, SUCH AS:

- Resistance to providing information necessary for starting a relationship or updating the registration;
- Providing false information;
- Providing information that is difficult or costly to verify;
- Opening, handling accounts or carrying out operations by holder of a power of attorney or any other type of mandate;
- Occurrence of irregularities related to the procedures for identifying and recording operations required by current regulations;
- Registration of several accounts on the same date, or in a short period, with deposits of identical or approximate amounts, or with other elements in common, such as origin of funds, holders, attorneys-in-fact, partners, address, telephone number, etc.;
- Operations in which it is not possible to identify the final beneficiary, observing the procedures defined in current regulations;
- Representation of different legal entities or organizations by the same attorneys or legal representatives, without reasonable justification for such occurrence;
- Information of the same residential or business address by natural persons, without demonstrating the existence of a family or business relationship;
- Incompatibility of the economic activity or billing informed with the pattern presented by customers with the same profile;
- Registration of the same e-mail or internet protocol (ip) address by different legal entities or organizations, without reasonable justification for such occurrence;
- Registration of the same e-mail or internet protocol (ip) address by natural persons, without reasonable justification for such occurrence;
- Information and documents submitted by the customer conflicting with publicly available information;
- Partners of companies without apparent financial capacity for the size of the declared business activity.

II - SITUATIONS ARISING FROM SITUATIONS RELATED TO PERSONS OR ENTITIES SUSPECTED OF INVOLVEMENT IN TERRORISM FINANCING AND THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION:

- Financial transactions involving persons or entities related to terrorist activities listed by the United Nations Security Council (UNSC);
- Operations or provision of services, of any value, to persons or entities that are known to have committed or attempted to commit terrorist acts, or participated in them or facilitated their commission;
- Existence of resources owned or controlled, directly or indirectly, by persons or entities that have been known to have committed or attempted to commit terrorist acts, or participated in them or facilitated their commission;

CHAPTER	04 - MONEY LAUNDERING PREVENTION AND TERRORISM FINANCING
SECTION	INSTITUTIONAL POLICY

- Transactions with evidence of terrorist financing;
- Financial transactions involving persons or entities related to the proliferation of weapons of mass destruction listed by the UNSC;
- Operations or provision of services, of any value, to persons or entities that are known to have committed or attempted to commit crimes of proliferation of weapons of mass destruction, or participated in them or facilitated their commission;
- Existence of resources owned or controlled, directly or indirectly, by persons or entities that are known to have committed or attempted to commit crimes of proliferation of weapons of mass destruction, or participated in or facilitated their commission;
- Transactions with evidence of financing the proliferation of weapons of mass destruction.

III - SITUATIONS RELATED TO EMPLOYEES, PARTNERS AND OUTSOURCED SERVICE PROVIDERS:

- Unusual change in the living standards and behavior of the employee, partner or outsourced service provider, without apparent cause;
- Unusual modification of the operating income of the partner's legal entity, including a correspondent in the country, without apparent cause;
- Any business carried out differently from the company's formal procedure by an employee, partner, included correspondent in the country, or outsourced service provider;
- Provision of assistance or information, remunerated or not, to a customer to the detriment of the company's money laundering and terrorist financing prevention program, or assistance in structuring or splitting operations, circumventing regulatory or operational limits.

IV - SITUATIONS RELATED TO OPERATIONS CARRIED OUT IN MUNICIPALITIES LOCATED IN RISK REGIONS:

- Atypical operation in municipalities located in border regions;
- Atypical operation in municipalities located in other risk regions.

Monitoring must cover operations and situations that appear to be related to other operations and related situations or that are part of the same group of operations.

V - BUYING OR SELLING GOLD OR OTHER PRECIOUS METALS:

Operations carried out with a legal entity whose representative is a PEP, accounts opened through a proxy, residents abroad and border regions will be identified for a specific analysis, focusing on risk and from the perspective of money laundering prevention and terrorism financing, as well as the verification of the origin of the resources, presumed financial capacity and the customer's tradition in the market.

CHAPTER	04 - MONEY LAUNDERING PREVENTION AND TERRORISM FINANCING
SECTION	INSTITUTIONAL POLICY

COMPLIANCE REPORT

After contextual and documentary examination, the Compliance department will record all actions in specific reports, which can be filed or forwarded for evaluation by the Risk and Compliance Committee, in relevant, atypical, or suspicious cases. The main objective of every analysis will be to identify possible situations in which there may be evidence of money laundering and combating the financing of terrorism.

COMMUNICATION OF SUSPICIOUS TRANSACTIONS

If LASTTRO TRADING suspects that the funds are the proceeds of criminal activity or are related to the financing of terrorism, the transaction or proposed transaction will be promptly communicated to the Financial Activities Control Council COAF (UIF) within 45 days after the decision is made known to the occurrence.

If LASTTRO TRADING suspects that the origin of the metal is different from that declared by the customer, or that the volume traded is greater than that considered feasible by LASTTRO TRADING, the company will notify COAF (UIF) under the same terms.

LASTTRO TRADING refrains from providing the respective customers or third parties with information on any communications made because of evidence of money laundering or terrorist financing.

LASTTRO TRADING, through the Risk and Compliance Committee, will deliberate on communications to COAF (UIF) in accordance with Resolution No. 23 of 12/20/2012.