# Banco de la República Oriental del Uruguay

## Anti-Money Laundering Unit

---

# *AML/CFT MANUAL*

---

**This manual does not modify nor replace any specific rules concerning products, services or procedures, which are to be applied in accordance with all its terms and conditions.**

Version 2018.1

## 1. INTRODUCTION

The Banco de la República Oriental del Uruguay (hereinafter BROU), as a financial intermediary institution in Uruguay, is obliged to apply a preventive policy intended to avoid its infrastructure being used for laundering monies

derived from illicit activities or for the financing of terrorism, under the national regulatory framework.

This Manual contains BROU's internal policies for the management of Money Laundering (hereinafter ML) and Terrorism Financing (hereinafter FT) risks assumed by the Bank.

## 1.1 Applicable regulatory framework

The Prevention Program adopted by BROU is suited to its operational procedures as a financial intermediary institution, in compliance with current laws and regulations, and the general rules and specific guidelines issued by the Central Bank of Uruguay (hereinafter CBU).
The Program has incorporated also the recommendations of the main entities specialized in this subject (FATF Recommendations, Basle Committee, Wolfsberg Principles), as well as the provisions concerning international banking relations (Patriot Act, OFAC Guidelines) applicable to financial intermediary institutions with the same operating features as BROU's.

## 1.2 Basic Concepts

### Money Laundering - Definition

Money laundering is a process through which criminal proceeds are incorporated into the legal financial system, disguised as licit.

In theory, the ML process has three stages: the placement of assets or funds; the transformation of funds to disguise their origin, ownership and location; and finally, the integration of funds.

### Money Laundering Process

### First Stage. Incorporation of assets or cash

This stage consists in introducing monies or other instruments into the financial system or in other sectors of the formal economy.
Throughout the process of legitimization of illegally obtained funds, the criminal organizations use a vast range of individuals, not only the players of the financial system, but other agents of the economy as well.

### Second Stage. Layering or Transformation

A series of operations are carried out in order to disguise or conceal the origin of funds, with the intention of removing traces and evidences.

### Third Stage. Investment, integration or possession of illicit funds.

This is the end of the process. At this stage, the monies laundered come back to the legal financial system, now disguised as "licit money".

## Financing of Terrorism - Definition

The FT crime is committed when a person organizes or, by whatever means, directly or indirectly provides or collects funds for the financing of a terrorist organization or a member of such an organization or an individual terrorist, with the intention of using said funds, or knowing that they will be used, in whole or in part, in the financing of terrorist activities.

Terrorist acts are crimes that are committed with the purpose of causing death or serious bodily injuries to a civilian or any other person that does not participate directly in hostilities in an armed conflict, when the purpose of this act, that is revealed by the nature of the act or its context, is to intimidate a population or to force a government or an international organization to act or to abstain from doing so. (International Convention for the Suppression of the Financing of Terrorism, adopted by the United Nations Organization).

## 1.3 Money Laundering Crimes

In articles 30-33 of Chapter V of Act 19.574 the Money Laundering crimes are categorised in the following terms:

> *Article 30. (Conversion and transfer) - The conversion or transfer of goods, products or instruments originated from any of the crime activities established in Article 34 of this Act shall be penalized to a jail term of two to fifteen years.*
>
> *Article 31. (Ownership and possession) - Any person who acquires, possesses, uses, has in their possession or carries out any type of transaction over goods, products or instruments originated from any of the criminal activities established in Article 34 of this Act, or that are a result of said activities, shall be penalized to a jail term of two to fifteen years.*
>
> *Article 32. (Concealment) - Any person who conceals, suppresses, alters the evidence or impairs the real determination of the nature, origin, location, destination, movement or beneficial ownership of said goods, products or other rights related to them originated from any of the criminal activities established in Article 34 of this Law shall be penalized to a prison term of twelve months to a jail term of six years.*
>
> *Article 33. (Assistance) - Any person who assists the agent(s) in the criminal activities established in Article 34 of this Law, whether it is to ensure the benefit or the result of said activity, to hamper the justice's actions or to avoid the legal consequences of their actions, or provides any help, assistance or advice, with the same goals, shall be penalized to a prison term of twelve months to a jail term of six years.*
> *This provision does not include the assistance or the advice given by professionals to their customers to verify their legal status or within the framework of the right of defense in legal, administrative, arbitral or mediation matters.*

Also, Article 34 in Chapter V of Law 19.574 defines criminal activities whose funds are object of Money Laundry:

> *Article 34. (Predicate offenses) - The following are the predicate offenses of money laundering, in their different modalities, as provided for in Articles 30 to 33 of this Law:*
> *1) Crimes provided for in Decree-Law 14.294 dated October 31st 1974 in wordings given by Law 17.016 of October 22nd 1988 and Law 19.172 of December 20th 2013 (drug trafficking and related crimes).*
> *2) Genocide, war crimes and crimes against humanity, categorized by Law 18,026 of September 25th, 2006.*
> *3) Terrorism.*
> *4) Terrorist Financing.*

*5) Smuggling of a real or estimate amount of over 200,000 UI (two hundred thousand index units).*
*6) Illicit trafficking in weapons, explosives, ammunition or weapon-usable materials.*
*7) Illicit trafficking in organs, tissues and medicines.*
*8) People smuggling and human trafficking.*
*9) Extortion.*
*10) Kidnapping.*
*11) Procuring.*
*12) Illicit trafficking in nuclear materials.*
*13) Illicit trafficking in works of art, animals or toxic materials.*
*14) Scam of a real or estimate amount of over 200,000 UI (two hundred thousand index units).*
*15) Misappropriation of a real or estimate amount of over 200,000 UI (two hundred thousand index units).*
*16) Offences against Public Administration, as provided for in the Criminal Code, Book II, Title IV, and in Law 17.060 of December 23rd, 1998 (public corruption crimes).*
*17) Fraudulent bankruptcy.*
*18) Fraudulent insolvency.*
*19) The offence provided for in article 5 of Law 14.095 of November 17th, 1972 (fraudulent corporate insolvency proceedings).*
*20) Crimes provided for in Law 17.011 of September 25th, 1998 as amended (trademark offences).*
*21) Crimes provided for in Law 17,616 of January 10th, 2003, as amended (intellectual property offences).*
*22) Criminal conducts provided for in Law 17,815 of September 6th, 2004, and in articles 77-81 of Law 18,250 of January 6th, 2008, and all those crimes provided for in the Optional Protocol to the Convention on the Rights of the Child, concerning child trafficking, prostitution or pornography, and human trafficking, smuggling or sexual exploitation.*
*23) Forgery and counterfeiting of currency, as provided for in articles 227 and 228 of the Criminal Code.*
*24) Receivership fraud, as provided for in Article 248 of Law 18.387 of October 23rd, 2008.*
*25) Tax fraud, as provided or in Article 110 of the Tax Code,*
*when the amount of the fraud tax or taxes in any fiscal year is over:*
*A) 2,500,000 UI (two million five hundred thousand index units) for years starting from January 1st, 2018.*
*B) 1,000,000 UI (one million index units) for years starting from January 1st, 2019.*
*Said amount shall not be required when using in total or in part, invoices or any other document logically or substantially false for the purpose of reducing the taxable amount or obtaining a wrongful tax return.*
*In the situations provided for in this item the tax fraud crime may be prosecuted ex officio.*
*26) Customs fraud, as provided or in Article 262 of the Customs Code,*
*when the wrongful amount is over 200,000 UI (two hundred thousand index units).*
*In this case the custom fraud crime may be prosecuted ex officio.*
*27) Murder committed as provided for in Article 312 Item 2 of the Criminal Code.*
*28) The bodily harm and grevious bodily harm crimes provided for in Articles 317 and 318 of the Criminal Code, committed as provided for in Article 312 Item 2 of the Criminal Code.*

*29) Theft, as provided for in Article 340 of the Criminal Code, when committed by an organized criminal group and whose real or estimate amount is over 100,000 UI (one hundred thousand index units).*
*30) Robbery, as provided for in Article 344 of the Criminal Code, when committed by an organized criminal group and whose real or estimate amount is over 100,000 UI (one hundred thousand index units).*
*31) Burglary, as provided for in Article 344 bis of the Criminal Code, when committed by an organized criminal group and whose real or estimate amount is over 100,000 UI (one hundred thousand index units).*
*29) Cattle theft, as provided for in Article 258 of the Rural Code, when committed by an organized criminal group and whose real or estimate amount is over 100,000 UI (one hundred thousand index units).*
*An organized crime group is a structured group of three or more people existing during a period of time and acting systematically with the purpose of committing said crimes, in order to directly or indirectly obtain an economic benefit, or any other material benefit.*
*33) Criminal association, as provided for in Article 150 of the Criminal Code. For the purpose of exchanging information between States, both by criminal legal cooperation and administrative cooperation between Financial Intelligence Units, the thresholds established in the previous items shall not apply.*

# 2. PREVENTION PROGRAM

## 2.1 Purposes of the Prevention Program

The following are the purposes of Banco de la República Oriental del Uruguay's Prevention Program:

- To establish control and prevention programs, policies and procedures that ensure complete compliance with the rules and regulations in force;
- To reassure customers that BROU applies the best prevention practices, in accordance with the highest international standards in this matter;
- To define and apply Customer Due Diligence policies and procedures, in order to know the beneficial owner of the accounts and transactions, as well as the origin of funds and securities;
- To implement policies and procedures regarding the Institution's staff that can guarantee their high level of trustworthiness, as well as their ongoing training in AML/TF;

- To maintain appropriate documentary backup to be used in need of reconstruction of the operations;
- To report unusual or suspicious transactions to the Financial Analysis and Information Unit (hereinafter UIAF, for its acronym in Spanish) in due time, according to the legal provisions in force and the regulations issued by the CBU.
- To comply with the obligation of reporting to the CBU's UIAF whenever the existence of assets related to terrorists or terrorist organizations is confirmed, according to the legal provisions in force and the regulations issued by the CBU.

## 2.2 Scope of Application

This Manual is applicable to all BROU branches within the national territory. as well as the foreign branches and the financial correspondents for the management of the Institution's customers. It should be known and applied by all employees, for every product and service provided by the Institution.

## 2.3 Contents of the AML Comprehensive Program

The Program is composed of the following elements:

- Prevention Structure
- ML/FT Risk Management System
- Customer Acceptance Policies
- Customer Due Diligence Policies and Procedures
- Transactions Monitoring Process
- Unusual and/or Suspicious Operations Report
- Financial Transactions Report furnished to the CBU
- Correspondent Bank policies and procedures
- Policies and Procedures regarding Staff

- Independent Review of the Prevention Program
- Prevention Manuals

# 3. PREVENTION STRUCTURE

BROU's Prevention Structure is composed of:

- Board of Directors of BROU
- AML Committee
- Compliance Officer
- AML Operational Committee
- Anti-Money Laundering Unit (hereinafter UPLA, for its acronym in Spanish)

## 3.1 Board of Directors

The Board of Directors is the highest AML authority within the Institution. The tasks of the Board of Directors are:

- Approving and adopting the Institution's Code of Ethics, ordering its compliance and circulation, and approving its updates.
- Approving UPLA's organizational structure.
- Appointing the Bank's Compliance Officer.
- Dealing with issues submitted by the AML Committee.
- Receiving the report presented by the Compliance Officer on an annual basis.
- Approving UPLA's Strategic Plan.
- Approving the AML Manuals.
- Ordering any measure deemed necessary within its tasks established in the Bank's Charter.

## 3.2 AML Committee

BROU has an AML Committee (hereinafter the Committee) which reports directly to the Board. This Committee is composed of two members of the Board, the General Manager and the Compliance Officer. One of the members of the Board acts as the Committee's President.
The Committee is in charge of planning, coordinating and monitoring the compliance with the Bank’s AML policies.

The tasks of the Committee are:

- Analyzing and approving the regular plans developed by the AML Unit (UPLA), as well as their level of compliance, notwithstanding the control carried out by the Audit Committee.
- Assessing, on a regular basis, the proper functioning of the AML Comprehensive Program.
- Being aware of the reports regularly issued by the Compliance Officer on the Bank's policies about compliance with laws and regulations, ethics standards, conflict of interest and investigations.

The Committee will gather on a quarterly basis or whenever its President may call for a meeting.

Apart from its members, the Committee may appoint employees to attend specific meetings if it deems their attendance relevant to discuss that meeting's agenda.

In each meeting, minutes shall be written up in order to specify the issues discussed, as well as the resolutions adopted and the matters that will require further treatment. These minutes shall be included in the Committee's Record of Minutes.

In order to open sessions, at least three members of the Committee have to be present.

In all cases, resolutions shall be agreed in writing and by unanimous decision of the members of the Committee attending the meeting. The matters that are not unanimously agreed shall be submitted to the Board of Directors for their consideration.

## 3.3 Compliance Officer

The Compliance Officer shall be in charge of proposing and developing the Institution's AML policies, and assessing their compliance by the Business Divisions, through the analysis of the procedures adopted for this purpose.

The tasks of the Compliance Officer are:

- Implementing the strategies and policies approved by the Board and developing well-documented procedures that allow to identify, measure and control the ML/FT risk, which shall be applied throughout the Institution, its subsidiaries and branches, as well as in the outsourced services;
- Verifying that the risks are framed within the levels established by the Board, or else are transmitted for their knowledge and decision by the corresponding management units;
- Assessing the efficiency of the AML/CFT Program, as per rules in force and according to the best practices in this matter;
- Proposing AML policies and procedures for the Institution;
- Giving advice to the AML Committee and other areas regarding AML/CFT;
- Fostering the adoption of the best AML/CFT practices within BROU;
- Verifying and coordinating the supervision and control of the AML/CFT Program in all BROU branches;
- Collaborating with the external agents in charge of the independent AML/CFT Program review;
- Acting as a link to competent authorities, and national and international related organizations;

- Supervising the correspondent banking relationships and AML due diligence in the Bank's branches abroad;
- Approving UPLA Policies and Procedures Manual;
- Reporting any suspicious operation (SAR) to the Financial Analysis and Information Unit and the General Manager.

## 3.4 AML Operational Committee

The AML Operational Committee (hereinafter the Operational Committee) is composed of the Compliance Officer, the Assistant General Manager of Sales and Distribution and the Executive Managers of the areas involved. In addition, depending on the issues under review, there may be other non-permanent members.

The tasks of the Operational Committee are:

- Making decisions regarding high ML/FT risk customers or customer groups, as well as those that do not comply with the rules.
- To make decisions on the inclusion or exclusion of persons in/from UPLA's Disqualified Persons List.
- Coordinating the necessary actions with the different areas involved in order to implement the decisions adopted by the Operational Committee.

The Operational Committee shall hold meetings on a quarterly basis or any time the Compliance Officer so requires. Every time a meeting is called to make decisions regarding the maintenance of business relationships with certain customers, said meeting shall be held within forty-five days from the relevant SAR.

Apart from its members, the Operational Committee may appoint employees to attend specific meetings if it deems their attendance relevant to discuss that meeting's agenda.

In each meeting, minutes shall be written up in order to specify the issues discussed, as well as the resolutions adopted and the matters that will require further treatment. These minutes shall be included in the Operational Committee's Record of Minutes.

In all cases, resolutions shall be agreed in writing and by unanimous decision of the members of the Operational Committee attending the meeting. The matters that are not unanimously agreed shall be submitted to the AML Committee for its consideration.

## 3.5 Anti-Money Laundering Unit

The tasks of the Anti-Money Laundering Unit (UPLA) are:

- Giving advice to the different services of the Institution in matters related to AML/TF.
- Developing the Institution's AML policies and procedures, following the goals set by the Board of Directors.
- Monitoring the effective implementation, by each Business Division and related services, of the rules and procedures adopted to prevent and control Money Laundering operations.
- Controlling that the policies and procedures adopted be reasonably suitable to prevent and spot money laundering and terrorist financing operations, in compliance with legal regulations in force and according to the best practices.
- Keeping the Bank's AML Policies Manual updated, submitting the proposed amendments to consideration of the AML Committee on a yearly basis.
- Developing AML training and awareness programs, in coordination with the Training Department, taking active part in their implementation.
- Centralizing the information and analysis of the Suspicious Activities Reports.

- Monitoring the efficiency and proper functioning of the automated alert system for detecting unusual operations (SAS).
- Reporting unusual or suspicious operations to the CBU, under the established procedure, and doing the follow up of said operations.
- Keeping the Risk Lists updated and carrying out the relevant controls.
- Reporting cash operations to the CBU, pursuant to the relevant regulations.
- Acting as a link to correspondent banks in order to request and/or send information about the application of AML policies and procedures.
- Taking part in seminars, courses or other internal or external training activities.
- Providing advice for the preparation of the Bank's Code of Conduct, in matters related to AML.
- Managing the definition and parameterization of the necessary alerts for the IT system.
- Developing and maintaining the ML/FT risk matrix.
- Coordinating and performing high-risk account monitoring or those established by the competent authority.
- Receiving, preparing and diligently processing the response to information requests from competent authorities, collecting and processing information through the Bank's operational services, within their respective confidentiality framework and in accordance with current regulations.

The structure of the Anti-Money Laundering Unit (hereinafter UPLA) was approved by Resolution of the Board of Directors dated September 27th, 2017.

## 3.6 Management standards related to money laundering and terrorism financing risks (ML/TF)

The Bank takes on a strong commitment in complying with the minimum management standards published by the Central Bank of Uruguay in force

since July 1st 2017 which establish the following aspects related to the money laundering and terrorism financing risks (ML/TF):

*MONEY LAUNDERING AND TERRORISM FINANCING (ML/TF) RISK*

*The risk of Money Laundering and Terrorism Financing refers to the possibility of loss or damage that an entity can suffer if it is used directly or through their operations as an instrument for money laundering and/or a resource channel towards terrorist activities, or when it is intended to conceal the assets resulting from said activities.*

*Money laundering operations are carried out for the purpose of legalizing (or at least appearing to do so) goods of an illicit origin; covering the illicit origin of the resources eliminating the connection with the activity that gave rise to them, or mixing illegal money with legitimate financial transactions for the purpose of justifying the origin of the total amount as resulting from a legal activity that serves as facade. By contrast, funds used to support terrorism may come from legitimate sources, criminal activities, or both. In this case what matters is to hide the source of financing, regardless if it is legitimate or illicit, since if it possible to cover the source, it will be available for future financing activities. Financial institutions have an important role, since criminal organizations or people will attempt to use them in many ways, from the introduction of cash to the legal circuit, carrying out multiple transactions or bank transfers to erase traces, transferring the safekeeping of securities and hindering the monitoring of illicit funds, to formally reinstate them in the legal circuit using the facade of a licit economic activity and developing normal transactions for any company, such as import, export, payment of services or interests on loans, but with the special characteristic of having an illegitimate and many times fictional origin.*

*Institutions shall implement a system that includes policies, practices and procedures that allow to identify, assess, monitor and mitigate the risk of being used as an instrument for laundering or channel of funds intended for terrorism financing. To do so, institutions shall have policies and procedures duly documented and communicated to all relevant staff, integrated in the general management of risks of the institution and applied continuously to the whole financial group. Strict rules to getting to know their customers shall be implemented, in order to identify who is the "real beneficiary" of the account. It is also necessary to establish ethical standards to ensure the integrity of the staff and to define continuous training programs for the employees in order to enable them to recognize the innovations related to these illicit actions and to proceed according to the situation. Also, the bank's commercial interests shall not be opposed at all with the efficient performance of the complying function. The entity shall assume a functioning and responsibilities structure according to its size and complexity of the operations and level of risk.*

*67. The Board shall approve the strategy and policies that promote a correct management of Money Laundering and Terrorism Financing risk on an individual and consolidated basis, and review them regularly. The Board shall regularly review the ML/FT exposure risk and ensure that the risk levels are within the established framework.*
*(…)*

*68. The High Management shall ensure the implementation of risk policies approved by the Board in relation to money laundering and terrorism financing risks, and the development of procedures to identify, measure, monitor and control.*
*(…)*

*69. The Compliance Officer is responsible for the implementation, follow-up and control of the correct operation of the ML/FT risk prevention.*
*(…)*

## 4. ML/FT RISK MANAGEMENT SYSTEM

The ML/FT Risk Management System (SARLAFT) analyzes, at least once a year, the inherent and residual ML and FT risk levels of the Institution's operations, assessing them in accordance with the Risk Management framework adopted by the Bank.

According to the best practices, the five Risk Factors (RF) identified and weighted in relation to the consolidated ML/FT risk of the Bank are: Customer, Product, Channels, Geographical Areas and Processes. Within said RFs, risk events are identified; for each event, the risk before controls (inherent risk), the existing controls and the risk after the control's impact (residual risk) are analyzed.

The Bank shall only carry out transactions or offer products or services when the associated ML and FT residual risk is "Low" or "Moderate".

The ML/FT Risk Management System shall be implemented in Uruguayan branches as well as in foreign branches.

## 5. CUSTOMER DUE DILIGENCE POLICIES

The beginning of the business relationship is the most appropriate moment to obtain the necessary information for the correct identification of customers, as well as to determine the purpose, nature and volume of the transactions that the customer is expected to carry out.

Notwithstanding the specific regulation provided for for the different products and operations, business units shall be specially cautious when accepting a

new business relationship. In this stage, it is very important that the employees in charge of admitting or approving a new business relationship, as well as those assisting in said task, pay careful attention to the information and documents provided by the potential customers. They are also responsible for the accuracy and integrity of loading data to IT systems and tools, as stated by the Bank.

BROU's prevention policy aims not only at the merely formal identification but also at getting to "know the customer". For this purpose, the employees who are in charge of customer admission or approval should obtain the necessary information and documents to verify the identity of the customer and the beneficial owner, make a reasonable assessment of the volume and nature of the customer's economic activity, understand customer's transactions and evaluate whether they are consistent with the nature and volume of customer's business.

Articles 6 and 7 of Law 19,484 establish the following in relation to the identification of the tax residence and final beneficiary:

> *Article 6 (Due diligence) - Financial entities bound to report pursuant to this law shall identify the residence for tax purposes of natural, legal personas or other entities that maintain accounts with them. The same requirement shall apply for the final beneficiary when applicable. (...)*
>
> *Article 7 (New accounts. Statement of tax residence) - Since the enforcement of this law, no new accounts may be opened, and no debt instrument or interest may be issued without complying, among others, with the requirement of stating to the financial entity the tax residence of individuals, legal entities or other entities and final beneficiary when applicable.*
> *(…)*

## 5.1 Purpose of Customer Due Diligence Process

BROU has adopted policies, procedures and controls in relation to Customer Due Diligence -based on its ML/FT risk assessment-, which aim at achieving the following goals:

- Identifying customers and verifying their identity, through documentary methods;
- Identifying the final beneficiaries and taking reasonable measures to verify their identity.
- Obtaining information about the purpose of the commercial relationship and the volume and nature of Customers' transactions;
- Being aware of the Customers' economic activity, business or profession, as well as the source of funds.
- Monitoring Customers' transactions in order to analyze whether they are consistent with the information that the Bank has of the customers.

## 5.2 Customer Acceptance Policy

It is BROU's policy not to establish or maintain commercial relationships with the following Natural and Legal Persons:

1. Natural Persons that have been accused or convicted of ML crimes by a national or foreign court, of which BROU has taken due knowledge. The AML Committee shall analyze their inclusion in UPLA's Disqualified Persons List. (*)
2. Natural Persons that have been accused or convicted of FT crimes, by a national or foreign court, of which BROU has taken due knowledge. The AML Committee shall analyze their inclusion in UPLA's Disqualified Persons List. (*)
3. Natural or Legal Persons included in the lists of the Office of Foreign Assets Control (hereinafter OFAC) or the United Nations Organization (hereinafter UNO).
4. Natural or Legal Persons, whether existing customers or would-be customers, not satisfying the Due Diligence requirements established by the Bank, as applicable.

5. Persons disqualified to operate with the Bank, by Resolution of the Board.
6. Persons included in UPLA's Disqualified Persons List, by resolution of the AML/FT Committee.

(*) In case a court has granted an acquittal to the defendant, or the case has been closed, thus being acquitted, the AML/FT Committee may establish an exemption to the general principle established in 1 and 2 above, after a risk assessment of the transaction proposed.
As for convicts, once they prove having served their sentence or that it has been suspended, the above procedure should be followed.

## 5.3 BROU Customers

BROU's regular customers are all those Natural and Legal Persons that have entered into a contract for the use of different products or financial services. Therefore, the Bank operates only with duly registered Customers that have satisfied all the requirements of the customer acceptance process, and all the conditions required for the use of the relevant product or service.
The Bank does not consider as customers those persons holding no account with the Bank and whose relationship with the Bank consists in doing the following transactions only:

| Transaction |
| --- |
| Payment of social benefits delivered by national public entities. (For example: Beneficiaries of Mides, Family Allowances, etc.) |
| Payments of funds or items managed by government offices, which the Bank is obliged to pay. (For example: Funds from the Ministry of Livestock, Agriculture and Fisheries (MGAP) |

| |
|---|
| Incoming transfers from abroad, whose ordering parties are foreign Social Security Organizations that have signed an agreement with BROU to pay their transfers, provided that in the payment details be stated that they are "PENSION, RETIREMENT OR RENT PAYMENTS" for amounts not exceeding: US$3,000 (three thousand US dollars) or its equivalent in other currencies. |
| Checks or Bills of Exchange issued by BROU, cashed at our counters. |
| Deposits to third party accounts |
| Other transactions made for account and by order of a customer. |

## 5.4 Walk-in Customers definition

Walk-in Customers are those who, over a calendar year period, make a series of occasional transactions, for an amount not exceeding: 305,000 UI or its equivalent in other currencies.

They can only be Natural Persons and their activity shall be restricted to currency exchange transactions and domestic money orders.

In case these customers begin to operate regularly or exceed the referred threshold, they shall be classified as Regular, and the Due Diligence procedures provided for in 5.5 shall be applied.

### Walk-in Customers Identification

To those Customers complying with the conditions specified in 5.4, at least the following information shall be required:

- Full name and surname;
- ID document number;
- Address and telephone number.

## 5.5 Regular Customer Due Diligence

Customer Due Diligence (hereinafter CDD) is applied to all Regular Customers of BROU.

To establish a relationship with a Regular Customer, besides satisfying BROU or CBU requirements, the following information and documents shall be required:

a)Natural Person

- The Customer should supply at least the following data:

  - ✓ Full name and surname;
  - ✓ Date and place of birth;
  - ✓ ID document number;
  - ✓ Marital status (married or cohabiting as per Law 18,246, and if so, name and ID document of spouse or domestic partner)
  - ✓ Address and telephone number;
  - ✓ Profession, trade or main activity;
  - ✓ Total income;
  - ✓ Country of residence;
  - ✓ Countries in which the Customer operates;
  - ✓ E-mail;
  - ✓ Statement certifying whether Customer is a PEP or not, and Customer's commitment to report to the Bank any related change;
  - ✓ Statement certifying whether the Customer operates on its own or for account of a third party, and if so, the Customer should state the identity of the beneficial owner;
  - ✓ Statement listing the products with which the Customer is going to operate.

- Copy of Customer's ID document (original must be submitted);
- Proof of Customer's address;
- Application Form for business relationship;
- Documents proving the existence of attorneys, if applicable;
- ID documents of the attorneys, if applicable;
- Registered signatures, if applicable;
- Documents proving Customer's business activity or profession and income, as applicable.

b)Legal Entities

- The representatives of the Legal Entity should provide, at least:

  - ✓ Name of the Legal Entity;
  - ✓ Date of Incorporation;
  - ✓ Address and telephone number;
  - ✓ Tax identification number;
  - ✓ Main activity;
  - ✓ Total income;
  - ✓ Country of origin;
  - ✓ Countries in which the Customer operates;
  - ✓ E-mail;
  - ✓ Statement certifying whether the Customer operates on its own or for account of a third party, and if so, the Customer should state the identity of the beneficial owner;
  - ✓ Statement listing the products with which the Customer is going to operate.

- Photocopy of RUT card or any other foreign tax identification document (CUIT, CGC, etc), showing the original document;
- Application Form for business relationship;
- Registered signature;
- Proof of address of the Legal Entity;

- Authenticated copy of the incorporation papers, by-laws or any other documentary proof of existence of the partnership, and proof of registration in the relevant register;
- Copy of documents certifying the legal capacity of representatives and attorneys (minutes of the board of directors, powers of attorney);
- Copy of the ID documents of the representatives and attorneys authorized to operate the account;
- Documents that allow to identify the shareholders or major partners, owners, or those who control the partnership. In all the cases, there should be a written document subscribed by the authorized signatures of the partnership, certifying the existence of shareholders or owners with a share of more than 10 pct of the equity capital and, if this is the case, identifying said shareholders.
- Supporting documentation related to the Customer's business activity and to the origin of funds, if applicable.

All Customer's representatives authorized to operate with the Bank should register their identification data as required under the Customer Acceptance Process. Also, the other members of the partnership (directors, partners, managers, etc.) should register their identification data according to the nature of their relationship with the Bank.

## 5.6 Customer Identification

### 5.6.1 Verification of customer's identity

During the customer acceptance process, the employees in charge shall determine and verify, based on documentary evidence, the customer's identity (holder/s), and in the case of a Legal Entity, the identity of representatives and attorneys (authorized to operate), and adopt reasonable measures to identify the beneficial owner of the funds, if applicable.

The Bank shall require the ID document of all the Individuals related to a customer: account holders, representatives, attorneys, beneficial owners, if applicable; a copy of said documents shall be retained in the Customer's File.

The ID documents should be issued by an official authority, be in force and have a photo of the individual requesting the Bank's services.

The documents considered valid are those defined by the CBU.

In the case of a Legal Entity, documentary evidence shall be required to prove its existence (certified copy of the incorporation papers or by-laws, proof of registration in the Public Registry of Commerce) and the legal capacity of its representatives and authorized employees to contract (Minutes of the Board of Directors, Powers of Attorney, i.a.), which shall be sent by the employee in charge of the relationship with the Customer to the Notary Department or hired Notary Public, as applicable.

The Notary Services Department or hired Notary Public shall analyze the referred documents and prepare a report including the following elements: name of the Legal Entity, legal form, date of incorporation, date of enrolment in the General Public Registry of Commerce, representation of the entity (stating capacity and identifying Representatives), identification of partners and their equity share (if stated in the Articles of Incorporation), among others.

After this stage of notarial analysis, the documents of the Legal Entity shall be kept by the Notary Services Department or the branch. The report prepared shall be sent to the employee in charge of the relationship with the Customer, to be included in the Customer's File.

## 5.7 Identification of Politically Exposed Persons

In the Customer Acceptance Process, it shall be stated whether the Customer is a Politically Exposed Person (PEP) and, in that case, it shall be included in the risk category generated by the Scoring tool. Notwithstanding this, and in compliance with the regulations issued by the CBU, all PEP's shall be subject to the enhanced due diligence procedures set out by BROU's internal rules.

The Bank has established two methods for the identification of PEP's: the Customer's testimony and the check on data bases of PEP's accepted by BROU.

## 5.8Business Activity of the Customer

BROU will try to gain an appropriate knowledge of the Customer, obtaining accurate information regarding the Customer's economic activity or profession and funds' origin, for the purpose of relating this information to the expected operations.

## 5.9 Enhanced Due Diligence

For customers rated as High ML/FT Risk and other risk groups, an Enhanced Due Diligence process should be carried out. To this effect, apart from applying the general Due Diligence procedure, some special requirements shall be imposed, according to the customer's activity and operations.

### 5.9.1 Correspondent Banking Relationships

#### 5.9.1.1 Correspondent Banks

BROU allows the establishment of correspondent banking relationships with domestic and foreign financial institutions.

As for the domestic financial institutions, said relationship shall be established under conditions that enable said institutions to maintain accounts or carry out payments or fund transfers for their own customers through our institution or vice versa.

As for the foreign financial institutions, the relationship is formalized through BROU's accounts with said institutions, intended for processing transfers or for carrying out investments of our own or for our customers.

The corresponding banking relationships shall be established only with entities that are effectively regulated and overseen in their country of residence. Therefore, to open and maintain a correspondent banking relationship, information should be obtained on the management, reputation and business nature (main activities, account purpose, geographical area of operation, i.a.) of the correspondent financial institution. Besides, before starting the relationship, the AML/CFT policies and procedures applied by the correspondent must be obtained and evaluated, in particular those concerning the acceptance and knowledge of the Customer.

No business relationship shall be established with correspondent financial institutions incorporated in jurisdictions that do not require a physical presence or with institutions that allow such type of entities to use their accounts.

Irrespective of the documents employed to define the responsibilities of each institution, especially those concerning the knowledge of the customer, BROU has adopted the Wolfsberg Questionnaire and the PATRIOT Act Form to exchange information with the correspondent financial institutions, for the purpose of collecting relevant information from a preventive point of view. Each Correspondent Institution File should contain the following details, i.a.:

- Institutional Data: Name, place of incorporation, branches, etc.
- Scope of the correspondent institution's activities
- Owners and managers data
- AML/CFT Controls
- KYC policies
- Transactions Monitoring

Furthermore, the Bank shall verify that the correspondent institution follows due diligence procedures, and that it has submitted the Audited Financial Statements (Audit Opinion included) of at least the last three fiscal years.

#### 5.9.1.2 Correspondent Financial Institutions

BROU establishes relationships with correspondent financial institutions that render authorized services in the country for account and under the responsibility of the Bank, within the Central Bank of Uruguay's regulatory framework.

The necessary actions shall be taken for the Correspondent Financial Institutions to apply the policies and procedures provided by the Bank, and to ensure the appropriate training in AML/CFT in relation to the contracted services.

The design and fulfillment of the services to be supplied by the Correspondent Financial Institutions shall ensure an appropriate monitoring and control of the transactions carried out, in compliance with current AML/CFT regulations.

### 5.9.2 Politically Exposed Persons (PEP's)

PEP's are those individuals who "are or have been entrusted with prominent public functions, domestically or by a foreign country, for example: Heads of State or Heads of Government, senior politicians, senior government, judicial or

military officials, important political party officials, directors and senior executives of state owned corporations and other public entities, as well as their relatives (parents, spouse, children) and close associates".

The relationships with PEP's, their relatives (parents, spouse, children) and close associates shall be subject to enhanced Due Diligence procedures, which should be applied, as a minimum, until five years after the politically exposed person has left office.

### 5.9.3 Regulated Institutions that manage funds on behalf of third parties

If the Customer manages funds on behalf of third parties, and is an authorized dealer in the exchange, banking, stock or insurance market, it shall be treated similarly to a High Risk customer. In this case, besides the information required to open an account for Legal Entities, the following information shall be also required:

- Procedures Manual or letter stating in detail the AML/CFT policies;
- Independent Review of the AML/CFT Program
- Additional information and document requirements of third parties whose funds are channeled through the Bank, as applicable, as per Art. 302 of the Compilation of Standards for the Regulation and Control of the Financial System (RNRCSF) - *Accounts opened or transactions related to individuals or entities that manage third parties' funds*.

### 5.9.4 Accounts used to channel third parties' funds

If confirmed that a Customer's account is regularly used to channel third party's funds, , measures shall be taken to verify that the Customer applies proper customer acceptance and due diligence procedures.

To this effect, the Customer shall provide information that allows to identify the client for which the Customer is operating (the Client of the Customer), and to determine the origin of funds.

Customers with activities included in Art. 302 of the RNRCSF - *Accounts opened or transactions related to individuals or entities that manage third parties' funds,* shall comply, as applicable, with additional information and document requirements of those third parties whose funds are channeled through the Bank.

### 5.9.5 Requirements for outgoing fund transfers

Before sending a fund transfer abroad, the Customer shall give instructions for the transfer, in the way and under the conditions established by BROU.

The ordering party, the beneficiary and the paying bank shall be checked against the lists of UNO and OFAC. No transaction shall be carried out if there is any true match with said lists.

If the transaction is made for account and by order of a third party, when instructed, the beneficial owner of the transfer (Client of the Customer) should be identified.

### 5.9.6 Requirements for incoming Fund Transfers

Our incoming fund transfers Service is rendered only to Regular Customers. When a fund transfer is received, it should be verified that the full details of the Ordering Party have been provided (full name, address and account number or ID number).

Special care should be taken with those incoming transfers that do not identify the ordering party as stated above. In such case, it should be evaluated if they are unusual or suspicious activities that require reporting.

When acting as intermediary, the Bank should keep Ordering Party's details during the whole payment chain.

The ordering party, the beneficiary and issuing bank shall be checked against the lists of UNO and OFAC. No transaction shall be carried out if there is any true match with said lists.

### 5.9.7 Fund transfers in general

International fund transfers in which the ordering party or beneficiary is an exchange house, financial service company or fund transfer institution shall not be processed.

BROU shall not participate in circuits of international fund transfer services from non-banking financial institutions.

For these purposes, those institutions which are not financial institutions but offer regular and professional domestic or foreign transfer and money order services are also deemed fund transfer institutions, notwithstanding their operational method (electronic transfers, instructions via phone, fax, internet, etc.).

## 5.10 Simplified Due Diligence

The Bank may establish simplified procedures of due diligence for customers, products and operations of low risk of money laundering or terrorism financing.

Simplified procedures shall be adjusted to the CBU's regulations.

When said measures are adopted, relevant controls shall be established in order to determine if an account or a customer does not have the features on which the application of the simplified measures was based. In such case, the additional due diligence procedures should be applied according to the new risk scenario.

Simplified CDD measures are not applicable when there is a suspicion of money laundering or terrorism financing.

## 6. TRANSACTIONS MONITORING PROCESS

BROU has implemented an automatic monitoring system of the transactions of its Customers, based on the best international AML practices.

## 7. UNUSUAL AND/OR SUSPICIOUS ACTIVITIES REPORT

### 7.1 Reporting Duty

For the purpose of complying with the provisions established in Article 12 of Law 19.574 and in Article 313 of the CBU's RNRCSF, any unusual or suspicious operation should be reported to the UIAF, under the conditions established in Communication N° 2008/214.

In this regard, the transactions considered suspicious or unusual are those -whether made or not- that, according to the usual customs and practice of the related activity, are unusual, have no evident economic or legal justification, or have an unusual or unjustified complexity; as well as those financial transactions that are suspicious of an illegal origin, pursuant to Uruguayan law.

### 7.2 Guide of unusual or suspicious transactions

### 7.2.1 Concept

For the purpose of collaborating in the process of detection of suspicious transactions by the legally bound subjects, CBU's UIAF publishes suspicious or unusual transactions Guides that compile types or patterns of financial transactions which might be linked to the legitimation of assets originated from criminal activities. BROU employees as well as those of financial correspondents providing services for BROU customers are required to be familiar with them.

## 7.3 Reporting on terrorism-related assets

As per the provisions of Article 314 of CBU'S Compilation of Standards for the Regulation and Control of the Financial System, the Financial Intermediation Institutions should report to the UIAF the existence of assets related to persons that are in any of the following situations:

- They have been identified as terrorists or as belonging to terrorist organizations, they are included in individuals or associated entities lists made up as per the Resolutions of the UN's Security Council, to prevent terrorism and its financing, as well as the proliferation of mass destruction weapons;
- They have been declared terrorists by a final judgment of a national or foreign court.

## 7.4 Legal regulations regarding legally bound subjects

Chapter II of Law 19.574 identifies legally bound subjects, both financial and non-financial, among which the Bank is included, who collaborate in the prevention system as follows:

*Article 12. (Legally bound financial subjects) - All natural or legal persons subject to CBU's control are legally bound to report the transactions, whether carried out or not, which according to the customs and practice of said activity are unusual or have no evident economic or legal justification or have an unusual or unjustified complexity. Those financial transactions involving assets suspicious of illicit origin should also be reported, in order to prevent the money laundering crimes under Articles 30-33 of this law, and to prevent as well terrorism financing. In this last case, the reporting obligation reaches even those transactions that - although involving assets of licit origin - are suspected of being related to individuals or legal entities involved in such crime or destined to the financing of any terrorist activity.*

*The information should be submitted to the CBU's UIAF, as they shall provide for.*

*The reporting obligation shall include the armored transportation companies as well.*

*The supervision of the activity of these legally bound subjects is in charge of the CBU.*

*The non-compliance with the reporting requirement shall determine the application, according to the case, of the sanctions and administrative measures provided for in Decree-Law N° 15.322 of September 17th 1982, as per Law N° 16,327 of November 11th 1992 and the amendments introduced by Laws N° 17.523 of August 4th 2002 and 17.613 of December 27th 2002.*

*Article 13. (Legally bound non-financial subjects) - The following subjects shall also be required to comply with the above obligation, under the same conditions:*

*A) Casinos.*

*B) Real estate agencies, real estate agents, construction companies and other intermediaries in transactions involving properties, except for leases.*

*C) Lawyers, only when acting in the name and on behalf of their customers in the following transactions, but in no event for any type of advice they give to their customers:*

*1) Promises, assignments of promises or sales and purchases of properties.*

*2) Administration of money, securities or other assets of the customer.*

*3) Administration of bank accounts, savings or securities.*

*4) Organization of contributions for the creation, operation or administration of partnerships.*

*5) Creation, operation or administration of legal entities, trusts or other legal forms.*

*6) Promises, assignments of promises or sales and purchases of commercial establishments.*

*7) Actions carried out by account of customers in any financial or real estate transaction.*

*8) Activities described in item H) of this article. As for the sale of legal entities, trusts or other legal forms, they shall be legally bound when acting in their own name as well as in name and for account of a customer.*
*D) Notaries or any other natural or legal person, when participating of the following operations for their customers, and in no event for any type of advice they provide:*
*1) Promises, assignments of promises or sales and purchases of properties.*
*2) Administration of money, securities or other assets of the customer.*
*3) Administration of bank accounts, savings or securities.*
*4) Organization of contributions for the creation, operation or administration of partnerships.*
*5) Creation, operation or administration of legal entities, trusts or other legal forms.*
*6) Promises, assignments of promises or sales and purchases of commercial establishments.*
*7) Actions carried out by account of customers in any financial or real estate transaction.*
*8) Activities described in item H) of this article.*
*E) Auctioneers.*
*F) Individuals or legal entities that carry out the intermediation or intervention in the purchase of antiques, artworks, precious stones and metals.*
*G) Operators and direct and indirect users of duty-free zones, as regards the uses and activities determined by the regulation.*
*H) Providers of corporate services and trusts and, in general, any individual or legal entity if they usually carry out transactions for their customers regarding the following activities:*
*1) Establishing partnerships or other legal entities.*
*2) Being a member of the Board or carrying out managing functions in a partnership, being a partner in an association or having similar functions in other legal entities, or appointing other person to carry out said duties, in the terms and conditions established by the regulations.*
*3) Providing a registered office or headquarters to a partnership, an association or any other instrument or legal entity, in the terms and conditions established by the regulations.*
*4) Carrying out fiduciary activities in a trust or similar legal instrument, or appointing other person to carry out said duties.*
*5) Carrying out duties of a nominal shareholder for account of another person, except for societies listed in a regulated market, subject to information requirements according to law, or appointing other person to carry out said duties, in the terms and conditions established by the regulations.*
*6) Sale of legal entities, trusts or other legal forms.*
*I) Civil associations, foundations, political parties, organizations and, in general, any non-profit association, with or without the status of legal entity.*
*J) Certified Public Accountants or any other individuals or legal entities, acting independently, participating in the following transactions for their customers, but in no event for any type of advice they provide:*
*1) Promises, assignments of promises or sales and purchases of properties.*
*2) Administration of money, securities or other assets of the customer.*
*3) Administration of bank accounts, savings or securities.*
*4) Organization of contributions for the creation, operation or administration of partnerships.*
*5) Creation, operation or administration of legal entities or other legal forms.*
*6) Promises, assignments of promises or sales and purchases of commercial establishments.*

*7) Actions carried out by account of customers in any financial or real estate transaction.*
*8) Activities described in item H) of this article.*
*9) Drawing up limited revisions of financial statements, in the terms and conditions established by the regulations.*
*10) Drawing up audit reports of financial statements.*

*Required subjects mentioned in items C), D) and J) of this article, are not under the obligation of reporting unusual or suspicious transactions, not even regarding the operations specified in said items if the information they receive from or through a customer was obtained to verify the legal status of their customer or within the scope of the defense right exercise in legal, administrative, arbitral or mediation matters.*

*The reporting on unusual or suspicious operations shall be addressed to the CBU's UIAF. This Unit, together with the National Secretariat for the Prevention of Money Laundering and Terrorism Financing shall establish how said reporting process shall be carried out.*

*(…)*

*The National Secretariat for the Prevention of Money Laundering and Terrorism Financing may require the legally bound subjects referred to in this article a regular reporting of any element deem useful to carry out its duties, and they shall be bound to provide it, otherwise the sanctions provided for in this article shall be imposed against them.*

*(…)*
*Article 21. (Record-keeping) - Legally bound subjects shall keep the records of all the transactions carried out with or for their customers, both domestic and international, including as well, all the information about customer knowledge obtained from the due diligence process, for at least five years after the business relationship is ended or after the date of the occasional transaction, or for a longer term of up to ten years, as established by the regulations.*

*The records on transactions and information obtained from the due diligence process must be sufficient to allow the reconstruction of individual transactions to provide, if necessary, evidence for prosecution of criminal activity.*

*These records and the information regarding customers and transactions must be available to the supervising authorities and the competent criminal court, upon their request.*

*Article 22. (Non-disclosure obligation) -Confidentiality is required. No legally bound subject, including those persons bound by contract, shall disclose to participants or third parties, the actions and reports carried out or produced about them, pursuant to the provisions of articles 6, 12, 13 and 26 of this law and the financial sanctions for the prevention and combat of terrorism and its financing, and for the prevention, elimination and cessation of the proliferation of mass destruction weapons.*

*Those who do not comply with this obligation shall be subject to the sanctions provided for in articles 12 and 13.*

*Upon receipt of the report, the UIAF may instruct the reporting person on the steps to be taken regarding the transaction in question and the business relationship with the customer. If within three business days the Unit does not give any instructions, the legally bound person may adopt the conduct deemed more suitable for their interests.*

*(…)*

*Article 23. (Disclaimer) - As long as the fulfillment in good faith of the reporting obligation provided for in articles 6, 12, 13 and 26 of this law and the financial sanctions for the prevention and combat of terrorism and its financing and for the prevention, elimination and cessation of the proliferation of mass destruction weapons, is in compliance with the relevant procedures established by the CBU or the Executive Power and in obedience to a legal provision enacted in the general interest (Article 7 of the Constitution of the Republic), it shall not constitute a breach of secrecy or confidentiality in any professional or commercial matter. Accordingly, it shall not produce any civil, business, labor, criminal, administrative or any other kind of liability.*

## 8. REPORTING FINANCIAL TRANSACTIONS TO CBU

As provided for in Article 550 of the Compilation of Standards for the Regulation and Control of the Financial System, the Financial Intermediary Institutions should report to the CBU all the information concerning Individuals or Legal Entities that carry out the following transactions:

1. Conversion of national/foreign currency or banknotes or precious metals into checks, transfers, bank deposits, stocks or other securities easily convertible, for amounts exceeding USD 10,000 (ten thousand US dollars) or their equivalent in other currencies;

2. Receiving and sending money orders and transfers, domestically and from abroad, for amounts exceeding USD 1,000 (one thousand US dollars) or its equivalent in other currencies, through whichever operating modality. Transfers and money orders made from one bank account to another shall be exempted from reporting in those cases where both accounts are held at local financial intermediary institutions;

3. Purchase and sale, exchange or arbitrage transactions in foreign currency or precious metals for amounts exceeding USD 10,000 (ten thousand US dollars) or their equivalent in other currencies, paid in cash;

4. Cash withdrawals for amounts exceeding USD 10,000 (ten thousand US dollars) or their equivalent in other currencies.

For transactions listed in 1 (deposits excepted) and 3 above, the information concerning those not exceeding the threshold amount should be reported if the total transactions made by the same Individuals or Legal Entities exceed USD10,000 or its equivalent in other currencies, in the course of a calendar month. As for bank deposits and cash withdrawals, the information to be reported shall refer to the total bank account movements over a calendar month, not to the Persons carrying out the transactions.

# 9. STAFF POLICIES

The implementation of staff policies aimed at reaching a high level of staff trustworthiness and ongoing learning and training in the prevention of ML/FT is one of the basic pillars of the Bank's Prevention Program.

## 9.1 Know Your Employee Policy

With regard to Prevention, the knowledge of the employees has a vital importance. For this purpose, BROU has adopted a series of measures intended to ensure a high level of employees' trustworthiness and adherence to institutional principles and values, through the dissemination of its Code of Ethics.
Financial correspondents providing services for BROU customers shall have policies in force consistent with this manual, in relation to: Code of Ethics, Staff Recruitment, Monitoring and Training.

### 9.1.1 Code of Ethics

All members of staff must duly comply with the provisions of the Code of Ethics, in conformity with the provisions of the Code of Good Practice of the Bank. To this effect, they are obliged to prioritize legality and ethical principles over mere

profit or the achievement of business goals. Likewise, they should avoid being in a position that may lead to a conflict between their personal interest and BROU's.

### 9.1.2 Staff Training

The Bank is committed to keep its staff duly trained and updated regarding the prevention of ML/TF.

The UPLA shall develop an Annual Training Program to be submitted for approval to the Compliance Officer who will report to the AML Committee.

Special training shall be offered for new employees of the Institution, and the needs that each sector may have shall be particularly dealt with, as per the assessment carried out.

A specific program intended for the specialization of all UPLA employees in this field shall be developed.

## 10. Independent Review of the Prevention Program

An external Audit Firm shall conduct an annual independent review of the AML/CFT Comprehensive Program. On the basis of said review, the Audit Firm shall submit a report to the Board of Directors of BROU, expressing their opinion on the suitability and proper operation of the control policies and procedures concerning the prevention of ML/TF. In their report, Auditors should state the most important deficiencies or omissions detected, as well as their recommendations to overcome said deficiencies, and the corrective actions adopted by the Bank.

## 11. PREVENTION PROGRAM MANUALS

UPLA is responsible for updating the following manuals, with the following regularity:

- AML/CFT Manual - annually
- Processes and Procedures Manual - annually
- FATCA Policies Manual - every four years