POLICY AND PROCEDURE FOR THE PREVENTION AND FIGHT AGAINST MONEY LAUNDERING, FUNDING OF TERRORISM AND PROLIFERATION OF WEAPONS OF MASS DESTRUCTION

This document defines the Policy for Prevention and Fight against Money Laundering, Funding of Terrorism and the Proliferation of Weapons of Mass Destruction in the Bank, explains the concept of Money Laundering activities, Illicit Acts and Funding of Terrorism and sets out the obligations for preventing such acts.

Given the serious consequences of Money Laundering, Funding of Terrorism and the Proliferation of Weapons of Mass Destruction in the Financial System, the bank "Banco Sol" considers that it is the duty of each of its employees, in their daily activities and within the scope of work, to be aware and comply with national and international laws, as well as internal policy guidelines related to this matter, in order to prevent the use of products and services made available by the institution for the purpose of these practices.

This Policy, as well as the following procedures, are applicable to all employees of Banco Sol.

- **National Regulation**

- Law 5/2020 of 27th of January – Law for the Prevention and Fight against Money Laundering, Funding of Terrorism and the Proliferation of Weapons of Mass Destruction.

- Law 1/2012 of 12th January – Law for designation and application of international acts.

- Law 3/2014 of 10th of February – Law for the Criminalization of B.C. Underlying Violations.

- Presidencial Decree 212/13 of 13th of December that sets out the Organization and Operation of the Finance Information Unit.

- Notice 14/2020 of 29th of May – Rules for the Prevention and Fight against Money Laundering and Terrorism Financing applicable by Financial Institutions supervised by the Banco Nacional de Angola (BNA).

- Notice 1/13 of 22nd of March, regulates the policies and procedures that the Financial Institutions must apply *as per* the Corporative Governance.

- Notice 2/13 of 19th of April, regulates the role of Compliance within the Internal Control System.

- Notice 6/2013 of 22nd of April – Remmitance of Funds Service.

- Directive 04/DSI/2012 of 24th July – Freezing of Funds and Economic Resources.

- Directive 03/DSI/2012 of 24th July – Identification and Reporting of Individuals, Groups and Designated Entities.

- Directive 01/2012 of 10th April – Reporting of Suspicious Operations of Money Laundering and Terrorism Financing.

- **International Regulation**

- 40 FATF/GAFI (Financial Action Task Force on Money Laundering) Recommendations published in 1990 and reviewed in 1996 and 2003 (including alterations of 22nd October 2004 to the 2003 version) on prevention and use of the international system as a means to carry out money laundering from illicit activities.

- 9 FATF/GAFI Recommendations, published in 2001 and reviewed in 2004, related to Fight against the Funding of Terrorism.

- Viena Convention: United Nations Convention against Illicit Drugs and Psychotropic Substances Traficking (1988).

- Palermo Convention: United Nations Convention against Transnational Organized Crime (2000).

- United Nations Convention on Money Laundering Suppression (1999).

- United Nations Security Council Resolution No. 1373 (2001) and United Nations Security Council Resolution No. 1267 (1999) and subsequent resolutions, related to the prevention and suppression of funding terrorist acts.

The Bank is committed to the highest standards of BC/FT/PADM and Compliance, providing employees with instructions and supporting tools to prevent the Bank being used as a vehicle for money laundering, terrorism funding and proliferation of weapons of mass destruction.

The standards set out by this Policy create a framework for the Prevention and Fight against Money Laundering Terrorism Financing and Proliferation of Weapons of Mass Destruction and are aligned with the internal structure and legal requirements and regulations. These standards are applicable to the Bank in the territories where it is authorized to carry out its activities.

For that, the Bank developed a program for the prevention and repression of Money Laundering, Terrorism Financing and Proliferation of Weapons of Mass Destruction, to guarantee that:

- All Bank customers and counterparts must be fully identified, the Know Your Customer (KYC) Diligence must be complied with and records of procedures carried out, must be kept;

- The Bank must fully comply with the applicable regulation, adhering to banking good practices in terms of identification of customers and counterparts, as well as financial operations carried out by them, for the Prevention and Fight against Money Laundering Terrorism Financing and Proliferation of Weapons of Mass Destruction;

- All areas direct or indirectly related with the activity must participate;

- A clear definition of procedures and responsabilities must exist;

- Training is given to Bank employees in order to facilitate a full and adequate compliance with the prevention program set out;

- Eventual signs of Money Laundering, Terrorism Financing and Proliferation of Weapons of Mass Destruction must be reported to competent authorities, in accordance with the applicable regulation;

- In short, to reduce the risk of the Bank being used for the practice of theses criminal activities contributing not only for the prevention of such activities and its social consequences, but also to protect robustness, integrity, stability, reputation and the image of the Bank;

It is the responsibility of the Executive Committee to define and implement and evaluate this program. For such purpose, the Executive Committee, has been indicated as the body responsible for overseeing, the program operational implementation and guarantee its compliance, the Compliance Directorate (*DCP*), in particular the Department for the Prevention of Money Laundering (*RPB*);

It is the responsibility of all employees to fully comply with the program in force.

The Bank guarantees that the program is available to all employees and any questions related to it can be answered, if necessary.

Every year or if required, depending on alterations made to the normative framework, implementation of the program will unergo an internal audit.

Periodically, i.e. anually or if required this Policy and Procedure for the Prevention and Fight against Money Laundering, Funding of Terrorism and Proliferation of Weapons of Mass Destruction will be fully reviewed.

According to the international standards, namely the ones related to the 40+9 FATF/GAFI recommendations and national legislation, money laundering has another crime in its origin. In fact, it is the process by which the products of the criminal activity are dissimulated to hide its illicit origin.

Thus, the money laundering can be defined as:

- Conversion or transfer of goods, when the person has the knowledge that these goods come from any violation or violations or the participation in this or these violations, with the objective of hiding or dissimulate the illicit origin of these goods or to help anyone involved in the practice of this or these violations, to escape the legal consequences of its acts;

- Hiding or dissimulating the true nature, origin, location, disposition, movement, ownership of goods or rights related to it, with the knowledge that they come from a violation or violations or the participation in this or these violations; or

- The acquisition, ceasing or use of goods, with the knowledge, at the time of its reception, that it comes from any violation or violations or participation in this or these violations.

On the other hand, the funding of terrorism can be defined as the supply or collection of funds, by any means, direct or indirectly, with the aim of using them or when there is knowledge that they can be used, in full or in part, in the planning, preparation or practice of a terrorist crime, i.e., the hijacking of hostages, tampering with administrative documents or the direction of a terrorist group, independent of the illicit origin of these funds.

Bearing in mind that the main methods used by these terrorist organizations for the transfer of funds between different locations are, in the main, similar to the ones used in the practice of money laundering crime, it is commom, particularly after the 11th September 2001, to consider jointly the Money Laundering Combat with the Funding of Terrorism. Such is the implicit understanding of this Policy.

Money Laundering or Funding of Terrorism include three phases (i) placement, (ii) circulation and (iii) integration, although with different meanings and scope.

In the beginning of the Money Laundering chain there are always illicit activities, whose generated funds are placed in any point of the legal financial and economic circuit (Placement). After that, transformation operations are executed and/or transfer of funds are introduced, in order to make the detection of the origin and tracking difficult (Circulation). Finally, the funds are forwarded to licit activities, namely for the acquisition

of luxury goods, non-fixed and fixed assets and for investing in economic activities (Integration).

Banco Sol complies with all the legal obligations and good practices, namely: Obligation of Risk Assessment, identification and due diligence, refusal, storage, reporting, abstention, cooperation and provision of information, confidenciality, control and training.

- **Risk Assessment Obligation**

The Bank must adopt measures to identify, assess, understand and mitigate the Risks of individual customers, transaction and Institution, bearing in mind the following:

- Nature, size and complexity of the activity developed by the entity in question;
- Countries or geographic areas in which the entity is operating, directly or through third parties, belonging or not to the same group;
- Business areas developed by the entity, as well products, services and avalilable operations;
- Nature of client;
- Background of client;
- Nature, size and complexity of the activity developed by the customer;
- Countries or geographic areas in which the customer carry out activity directely or through third parties, belonging or not to the same group;
- Type of the business partnership set up;
- Geographical location of customer of the entity responsible or where it is based or in some way develops its activity;
- Transactions carried out by the customer;
- Network of distribution of products and services available, as well as the means of communication used to contact customers.

For the purposes set in the previous number, the Bank must develop and implement tools and/or systems of information for the efficient management of the risk of Money Laundering Combat, Funding of Terrorism and Proliferation of Weapons of Mass Destruction.

The nature and size of the risk assessment must be adequate to the characterisitics, size andcomplexity of our institution.

Elaborated by:	DIRECTORATE OF INSTITUTIONAL DEVELOPMENT	Elaboration Date :	28-05-20
Approved by:	EXECUTIVE COMMITTEE	Approval Date:	

The appropriate measures mentioned on number 1 *supra*, must include:

- Documentation of risks inherents to specific operation environment of the entity and how it has been identified and assessed, as well as the adequacy of the means and the control procedures used for the mitigation of identified and assessed risks on how the entity monitor the adequacy and efficacy of theses means.
- Consideration of all relevant risk factors before determining the global risk level and the adequate type and size of mitigation measures to be applied;
- Ongoing update of risk assessments of institution being assessed;
- Use of appropriate technical and technological mechanisms to provide information on risk assessment to the relevant authorities;
- Demonstration of the adequacy of procedures adopted, upon request by the relevant supervisory or overseeing authority.

The Bank must also:

- Develop and implement the internal policies, procedures and controls approved by the correspondent managing body, in order to facilitate the management and mitigation of risks identified or that have been reported to the relevant authorities;
- Monitor and implement such procedures, controls and policies and improve them, if necessary;
- Apply robust management measures and efficient mitigation of identified high risks, when they are identified and simplified measures if risks are low;
- Guarantee that the application of above mentioned simplified or reinforced measures, addresses the risks assessment and the guidelines of the supervisory and overseeing authorities.

Identification and Diligence Obligation

The Bank ensures full Identification and Due Diligence of client and if applicable, of the legal representatives and the effective beneficiary, whenever:

- Business relationships are set up;
- Random transactions are carried out:

Elaborated by:	DIRECTORATE OF INSTITUTIONAL DEVELOPMENT	Elaboration Date :	28-05-20
Approved by:	EXECUTIVE COMMITTEE	Approval Date:	

i. With an amount equal or above the value of USD 15 000, equivalent in the national currency or in another currency, independent of being or not a single operation or being an integral part of many aparently linked operations;
ii. Any wire transfer with an amount equal or above the equivalent, in national currency or any other foreign currency;

It is suspected that there a crime of Money Laundering, Funding of Terrorism and Proliferation of Weapons of Mass Destruction; and,

There are questions about the authenticity or the compliance of customers identification data previously obtained.

The Due Diligence measures to be taken and related to the customer are the following:

- Identify and verify the customers identity and their representative:
  i. For individuals, the identity verification must be made through the presentation of a valid official document showing photograph, full name, signature, address, DOB and nationality;
  ii. For corporate accounts the identification is made through the presentation of original document or photocopy of the public deed of incorporation or equivalent document, certificate of incorporation, publication in the Official Gazette, licenses, valid license issued by a competent authority and the tax number;
  iii. In case of non resident corporate account holders, the identification is made through an equivalent document;
  iv. Identification of unincorporated collective entities set up in accordance with foreign law or similar legal tools, must include obtaining and verifying the name of the trustees, settlors and beneficiaries.

- Identify and verify the actual beneficiaries, using information from credible sources, requiring at least, the following information:

  i. Authenticated document confirming the identity of the actual beneficiary;
  ii. Copy of the fiduciary agreement, company statutes or other equivalent document;
  iii. Minutes of the Constituent General Meeting, as well as the minute of the alteration of the company ownership structure or its stakeholders;
  iv. Other reliable and public available information and a relevant banking institution;

Obtain information about the objective and nature required for the business partnership;

i. Obtain information related to customers that are companies and unincorporated collective entities to help in understanding the nature of customer business, the stake in the control of the share capital, names of members of management bodies;
ii. Obtain information, on the origin and destination of funds movements, when customer risk profile or characteristics of the operation justifies, *as per* the scope of a business partnership or the occasional execution of a transaction and request supporting documentation;
iii. Follow up continually the business partnership, in order to ensure that such operations are consistent with the knowledge that the relevant entity has in its records regarding the client, its dealings and risk profile;
iv. Keep up to date information obtained in the course of the business partnership;

- Whenever the relevant entity is aware or suspects that the customer does not act on its own, adequate measures must be taken to help with identifying of the person or entity that is working on behalf of the customer, namely the effective beneficiaries;
- The relevant entities must also verify if the clients representatives are legally entitled to act on their behalf or represent them;
- The obligation of identification set out in Number 2 of this Article, must be applied to existing clients and the verification of their identity will be subject to regulation issued by the supervisory and overseeing authorities.

The bank does not establishes a business partnership or carry out any occasional transaction, if the identification duty has not been complied with, except if it is proven to be indispensable for the execution of the operation and in this case the identification procedures will be complied with in a shorter period of time.

Bank does not allow any debit or credit transaction in the account, after the initial deposit and does offer any payment facilities for the account or change of ownership, without previous verification of the customer identity *as per* applicable legal or regulatory provisions.

Bank applies Due Diligence procedures regularly and this is depending on the existing level of risk, to new and existing customers.

Bank registers and saves in the activities supporting system all customers data that are considered significant. Further eventual risks are also recorded for the use of the Bank for Money Laundering and Funding of Terrorism operations.

Among other deemed necessary actions, the Bank will carry out background checks to identify if the customer name is blacklisted and will seek to obtain information on the customer reputation, origin of funds and objective of the operation.

The Bank will not initiate a business partnership, if it cannot obtain all the necessary information or if the information available indicates that it must not do so.

It is the duty of the Bank, however, to demonstrate that the procedures adopted are adequate.
As per in force law and good practices, the Bank may simplify or reinforce its Due Diligence duty.

- **Refusal Obligation**

Without prejudice of the right of communication and in case the requirements set out in Articles 11 and 14 of the law cannot be complied with, the Bank must:

- Refuse to open an account;
- Refuse to initiate the business Partnership;
- Refuse to carry out transactions;
- Terminate the business Partnership.

If one of the above mentioned options occurs, the relevant entity must review the circunstances behind the occurrence and if there is a suspicion of the practice of a crime of Money Laundering, Funding of Terrorism and Proliferation of Weapons of Mass Destruction, they must report it *as per* applicable law and think about terminating the business partnership.

- **Storage Obligation**

The Bank stores for a period of 10 (ten) years, starting from the moment when the transaction is carried out or after the end of the business partnership, at least, the following documents:

- Copies of documents or other digital information as proof of compliance with the identification obligation and that of Due Diligence, including the storage of records on customers classification;
- Records of transactions, including all the original information together with transaction beneficiary, to permit the reconstitution of each operation, in order to provide a proof, if necessary, within the scope of a criminal process;
- Copy of all the business correspondence exchanged with client;
- Copy of communication between relevant entity and Financial Information Unit and other competent authorities;

- Internal analysis results records, as well as the record of the reason for the decision of relevant entities in order not to report these results to the Financial Information Unit or to other relevant authorities;
- Information explained in the previous entry above must be available for the Financial information Unit and other competent authorities;

- **Reporting Obligation**

The Bank, by its own accord, informs immediately, the Financial Information Unit, whenever it is aware or has enough reasons to suspect that occurred, is in course or there was a certain operation attempt, to be associated with the practice of Money Laundering, Funding of Terrorism and Proliferation of Weapons of Mass Destruction or any other crime.

For the purposes set in the previous number the operation may involve a single transaction or be an integral part of a set of transactions aparently not linked to each other.

The relevant entities must report to the Financial Information Unit, all the transactions in money that are equal or above in national currency or other equivalent currency, as established by law and shown in the table annexed.

- **Abstention Obligation**

If the Bank identifies a specific transaction showing signs of being suspicious and is linked to the practice of the crime, the relevant entity apart from having to comply with the obligations set out by Articles 11 to 14 of Law 05/2020, must refrain from carrying out any operations associated with the customer.

For the purposes set in the previous number, the relevant entity must immediately, inform in writing or by any other mean the Financial Information Unit, the reasons behind the suspicion and request confirmation of suspension of operations.

The Financial Information Unit must confirm the suspension of operation within 3 (three) working days from the date of reception of the information, at the end of which, if not confirmed, the operation can be completed.

If the relevant entity considers that the abstention mentioned in point one is not viable or that, after consulting with the Financial Information Unit, may be prone to hamper the prevention or the future investigation of Money Laundering and the Funding of Terrorism or the Proliferation of Weapons of Mass Destruction, the stop to the operation must be executed and in this case the relevant entity must supply immediately to the Financial Information Unit, all data associated with the operation.

When the suspicion is confirmed, the Financial Information Unit must request to the Public Prosecutor the approval of the decision of suspension of operation within a maximum of 7 (seven) working days from the date of the decision referred to in point 3.

The Public Prosecutor must within 10 (ten) working days reach a decision on approving the decision of suspension of operation within 7 (seven) working days from the date of decision referred to in point 3.

The Public Prosecutor must reach a decision within 10 (ten) working days from the date of the Financial Information Unit request.

In case the Public Prosecutor does not approve the suspension, the Financial Information Unit communicates immediately this fact to the relevant entity in order to carrry on with the operation.

In case the Public Prosecutor does not take a decision within the timeframe indicated in point 6, the Financial information Unit communicates immediately to relevant entity that can execute the operations to which the duty of abstention was applied.

- **Cooperation and Provision of Information Obligation**

The Bank must promptly cooperate and provide information to the Financial Information Unit, supervisory and overseeing authorities and when requested by these, provide information on operations carried out by customers and show the documents of such operations;

The Bank must have in place systems and instruments to respond promptly and fully to information requests presented by the Financial Information Unit and other competent bodies, in order to establish if they maintain or maintained, within the last 10 (ten) days, a business partnership with a specific person or group of people and the nature of these partnerships;
The Bank must also cooperate and provide all the data requested by competent legal authorities;

- **Confidentiality Obligation**

The Bank and members of respective company bodies or, executives, managers or team leaders, employees, representatives or other people that provide services, either permanent, temporary or occasional, cannot disclose to customer or to third parties, that they have disclosed the information required by law or that there is an ongoing investigation process.

- **Control Obligation**

The Bank must implement adequate programs of Prevention and Fight against Money Laundering, Funding of Terrorism and Proliferation of Weapons of Mass Destruction, adapted to the activity sector, respective risk and size of the business activity in question, including the following policies, procedures and internal controls:

- Compliance control systems, including the appointment of an executive;
- An independent internal control structure to test the system of Prevention and Fight against Money Laundering, Funding of Terrorism and Proliferation of Weapons of Mass Destruction;
- Definition of an effective risk management model that includes identification, assessment and risk mitigation for Money Laundering, Funding of Terrorism and Proliferation of Weapons of Mass Destruction that the relevant entity is or may be exposed to;

Financial groups and similar of non financial institutions have the obligation of developping programs to fight Money Laundering, Funding of Terrorism and Proliferation of Weapons of Mass Destruction at a group level, that must be applicable and adapted to all the main subsidiaries and branches;

The programs referred to above must include the measures as well as:

- Policies and procedures for sharing of information as required for compliance with duty of identification and Due Diligence of customers and for the risk management of Money Laundering, Funding of Terrorism and Proliferation of Weapons of Mass Destruction;
- Provision of information at a group level, associated with compliance control, auditing and/or the Fight against Money Laundering, Funding of Terrorism and Proliferation of Weapons of Mass Destruction;
- Provision, when necessary, of information about customers, accounts and operations of subsidiaries and branches for the Fight against Money Laundering, Funding of Terrorism and Proliferation of Weapons of Mass Destruction;
- Guarantee the confidenciality and the good use of shared information;

The Bank must apply measures of Prevention and Fight against Money Laundering, Funding of Terrorism and Proliferation of Weapons of Mass Destruction *as per* obligations of Law 05/2020, to main subsidiaries, branches and partners, based abroad, where the host country minimum requirements are not robust, as long as their Law and regulations allow;

If the host country does not allow the application of the above mentioned provision, the [entidades sujeitas] are forced to apply effective additional measures, in order to manage the risk of Money Laundering, Funding of Terrorism and Proliferation of Weapons of Mass Destruction and inform the supervisory and overseeing authorities.

- **Training Obligation**

The Bank must guarantee provision of regular and effective training for employees, executives and managers, in compliance with the obligations enforced by current Law and regulations for the Prevention and Fight against Money Laundering, Funding of Terrorism and Proliferation of Weapons of Mass Destruction and inform the supervisory and overseeing authorities.

The Bank must store, for a period of 5 (five) years, copies of documents or records of training provided to employees and managers.

Penalties

Non compliance with the above are punished in accordance with the following terms:

- When the non compliance occurs within the scope of a financial institution activity:
- With a fine between the amount of Akz 45,645,800.00 (fourty five million, six hundred and forty five thousand and eight hundred Kwanzas) and Akz 4,564,580,000.00 (four billion, five hundred and sixty four million and five hundred eighty thousand Kwanzas), if the agent is a company; and;
- With a fine between the amount of Akz 5,705,725.00 (five million, seven hundred an five thousand and seven hundred and twenty five Kwanzas) and AKz 1,141,145,000,00 (one billion, one hundred and forty one million and one hundred and forty five thousand Kwanzas), if the agent is a single person;
- When the non compliance occurs within the scope of a non financial institution activity;
- With a fine in the amount of Akz 2,282,290.00 (two million, two hundred and eighty two thousand and two hundred and ninety Kwanzas) to Akz 1,141,145,000.00 (one billion, one hundred and forty one million and one hundred and forty five thousand Kwanzas) to 456,458,000.00 (four hundred and fifty six million and four hundred and fifity eight thousand Kwanzas) if the agent is a single person.

Further Sanctions

Jointly with penalties, the following further sanctions can be applied to the person responsible for any non-compliance *as per* the Article 72 of Law 05/20, depending on how serious the non-compliance is and how deep is the involvement of the agent:

- Warning, applicable once;
- Prohibition, for a period of up to 3 (three) years of professional practice or activity associated with the offence in question;
- Inhibition, for a period of up to 3 (three) months to 3 (three) years on carrying out social duties or being appointed to administrative, management, leadership and supervisory roles in companies subject to current law, when the offender is a member of the company board and act as executive, leader or manager or as a legal or voluntary representative of a company.
- Permanent prohibition to carry out a job or activity associated with the offences, the social role or supervisory duties in companies referred to in the previous point;
- Publication of the permanent prohibition and costs incurred by the offender in a daily print national newspaper.

INTERNAL PROCEDURES

1. Identification and verification of Clients

Considering that to know the Customer is a fundamental tool in the fight against the use of the financial system for Money Laundering, Funding of Terrorism and Proliferation of Weapons of Mass Destruction, the Bank is commited to initiate a business partnership with Customers that provide the required information and in accordance with the Law and after the analysis of such information.

For such purposes the Bank holds a customers identification manual and developed an opening account process to easily obtain and register identity, representations, address, legal capacity, occupation or Customers social object, as well as other identification data, that must always be carefully identified against original documents or certified copies, whose counterparts the Bank must keep.

The Bank applies regularly Due Diligence procedures, not only to new Customers but also to existing ones depending on the existing risk level.

The minimal data required for the identification of clients are as follows:

Individuals

a) Surname and names;
b) Date and place of birth;
c) Marital status;
d) Full address or, if it is not possible, any other contacts considered valid;
e) Number of ID used, expiry date and issuing authority;
f) Professional status and employer identification (if applicable); and
g) Origin and nature of funds involved in the business partnership or transaction.

Companies

a) Name of company;
b) Company object;
c) Headquarters address;

d) Company´s incorporation details;
e) Tax Number;
f) Commercial Tax Number;
g) Purpose and object;
h) Legal and stakeholders structure; and
i) Origin and nature of funds involved in the business relationship or transaction.

The Norm PCN.ABR.03 – Account Opening, as well as the corresponding opening account checklists explain the internal norms regarding this topic.

When there is a suspicion or certainty that a customer does not act alone, enough information must be gathered to verify and record the identity of representatives, solicitor or nominee, as well as the people on behalf of whom they act for.

The Compliance Officer may determine that additional information must be obtained when the Customer has an activity considered potentially risky, taking into account the KYC information.

Efective Beneficiaries (BEF's)

Whenever there are reasons to believe that a Customer does not act in his own behalf, his information must be obtained and the transaction or asset actual and effective beneficiary identity must be verified.

The Bank identifies not only its Customers but also its representatives and, if necessary, the effective beneficiaries, requesting the same elements and identification documents that would otherwise request to the Customer.

The effective beneficiary is a single person, that in the last instance controls the customer, or in the name of whom a certain transaction is carried out.

The person or single entity that:

- Have, ultimately, a share in the capital of a company or control and/or the single entity in which name the operations have been carried out;
- Have, in the last instance, an effective control of the company or unincorporated entity in those situations where the share in the capital/control is made by means of a chain of shares in the capital or through an indirect control;
-

- Have, in the last instance, the asset or the direct or indirect control of the share capital or the voting rights of the company, is not a company listed in the stock exchange, subject to requirements of information that comply with the international norms;
- Have the right of exert or that exert significant influence or controls the company independent of the level of participation;
- In case of legal entities that administer or distribute funds, the person or people that:
- Benefit from its assets when the future beneficiaries have been determined.
- Seen as a category of people whose main interest the company was incorporated or exert its activity, when future beneficiaries have not been yet determined;
- Exert control of the assets of the company.

Risk Countries

Some countries may be qualified as "Risk Countries", because of the political disturbances, armed conflicts, high level of organized crime, known involvement in the production or traffic of drugs, etc.

Maintain commercial dealing with citizens from Risk Countries, with people based in that Risk Country or that maintain regularly a commercial activity with this type of countries, may expose the Bank to a major risk. Subsequently, the Bank filters the information linked to Customers and operations against lists of sanctions (including the UN, *OFAC*, *HMT* and *CFSP*)*, PEP's and adverse information.

Politically Exposed Person (PEP's)

As per the Law 05/2020, the people in this category bear an added risk in terms of Money Laundering, Funding of Terrorism and Proliferation of Weapons of Mass Destruction, that justifies the implementation of more robust procedures of analysis and knowledge of the Customer – Robust Due Diligence duty.
Politically Exposed People (PEP's) are those national or foreign individuals that carry out or carried out proeminent public roles in Angola, or any other Country or Jurisdiction or in any International organization.

The Bank defines PEP's as the accounts in which any of its intervenients identified in opening account documents are included in this category. In these cases, the following procedures are adopted:

- The Bank will request aditional information, namely, the origin of assets and funds involved in the business partnership or other information considered relevant.
- The opening of any account by a PEP must be approved by the Executive Committee. For this, the Compliance Officer is responsible for the elaboration of a report that is presented to the Chief Financial Officer, who submits to the Executive Committee for respective account opening authorization.
- The Executive Committee must take a decision on opening an account within a maximum of 48h, from the time the Compliance report submission occurred.
- A minute is drawn up with the decision of the Executive Committee and signed by all present in the meeting and that will be archived in an appropriate book.
- The department of Account Maintenance is responsible for guaranteeing that the customer classified as PEP will not be allowed to use the account until the Compliance Directorate report the authorization to the Executive Committee.
- If in the course of the commercial relationship with the Bank, an account holder at a specific moment is classified as PEP, the Customer Banking Advisor aware of this fact, must immediately update the Client corresponding KYC.
- The relationship that the Bank creates with PEP's Customer will be reviewed quarterly by the Customer Bank Adviser with the supervision of respective Director. In case the political framework, the position of the Customer or the nature of the actual relationship with the Customer changes considerably, the Compliance Officer must be informed immediately and a full and global reassessment of the process of this Customer will be carried out.

The Compliance Directorate is responsible for the ongoing monitorization of operations linked to PEP's accounts. For this, it will receive a report of operations or transactions that are destined or have been requested for PEP's accounts.

The Compliance Officer is responsible for elaborating a monthly report of activity for PEP's accounts.

3. Non-profit Organizations

Given the risk of Money Laundering and Funding of Terrorism that these bodies are under because of the nature of its activities, the Bank considers that they must undergo a more robust Due Diligenge.

Thus it up to the Compliance Directorate to collect additional information namely, locations of operation, organization structure, nature of donations and volunteering, as well as the nature and beneficiaries of funds.

The Compliance Directorate is equally responsible for elaborating an opinion about the opening of the accounts for clients classified as non-profit organizations.

3. Banking Correspondence Liaisons

Banking Correspondence Liaisons include a high risk for the Bank that must be taken into account through the execution of robust measures of Due Diligence to mitigate the risk, namely through:

a) Collection of information on the nature of the correspondent bank activity, internal control processes for Money Laundering and Funding of Terrorism, ensuring adequacy and efficaccy;
b) Appreciation, based on publically known information, correspondent bank reputation and supervision characteristics including, for example, the Bankers Almanac platform as a reference source;
c) Previous authorization from Executive Committee and Bank Board of Directors of the correspondent banking relationship;
d) Written description of respective responsibilities whenever the Bank establishes a correspondent relationship involving institutions based in third party countries.

Procedures for the monitorization of correspondent banking activities were implemented:

a) Request for the identification of the Country of origin of the correspondent Bank in question and verification of the additional risk;
b) Request for policies and internal procedures of the correspondent Bank for the Fight Against Money Laundering and Funding of Terrorism;
c) Request for policies of identification and acceptance of customers of the correspondent Bank, in order to verify the procedures regarding the permission for opening anonymous accounts and/or with ficticious names;

d) Verify and review the information reported using the existing media, in order to ascertain the reputation of the correspondent Bank in question;
e) Every year and if necessary, the Compliance Directorate jointly with the Investment Banking Directorate, request to the correspondent Bank the up to date information described in the above mentioned procedures;

4. Identification and Verification of Counterparts Associated to Occasional Transactions

By Law, the Bank must identify and verify the identity of payers whenever they execute occasional transactions equal or above an amount of USD 15000.

A transaction is considered occasional when it occurs outside the scope of an already established business partnership.

In order to comply with the Angolan Legislation, the Bank has determined that all payers, either Bank customers or not, that deposit cash equal or above the amount of USD 15 000 or equivalent in Kwanzas, must be identified through the presentation of an ID at the time when the deposit is made. This information must be registered in the Declaration of Origin and Destination of Funds that must be filled in at the moment of occurrence of the transaction and signed by the depositor.

a) In the internal Norm PCN.DNU.01 – Cash Deposits, shows in detail the procedures related to cash deposits.

5. Control and Storage of Documents

The Customer Bank Advisor is responsible for gathering all the documentation necessary for the opening of accounts including the filling up and signing of forms. Ultimately, the Accounts Maintenance Department verifies the compliance with the requirements for the account openings.

In case there is a missing document in the file, the Compliance Officer may, exceptionally, authorize the account opening. If the Compliance Officer authorizes to open the account without meeting the required requirements, it will always submit a short justification.

6. Control and Storage of Documents

The Customer Bank Advisor is responsible for obtaining all the documents necessary for the account opening, including the filled up and signed forms. Ultimately, it is up to the Accounts Maintenance Department to verify the compliance of the requirements for opening accounts.

If a document is missing in an application file, the Compliance Officer will, exceptionally, authorize the opening of the account. If the Compliance Officer authorizes to open the account without meeting the requirements, it will always submit a short justification.

Within the scope of control, in relation to account opening, the Compliance Officer will monitor all the issues of missing documentation, as well as the update of Customers data, for that, the department of Account Maintenance will send to the Compliance Directorate a monthly report on the documentation status for the opening of new accounts. After the review of information, the Compliance Officer will determine the closure of the account that does not meet the requirements.

The Bank will archive all the documentation gathered for the account opening and for carrying out the operations.

At least the following documents will be kept for a period of 10 years, from the moment the transaction is carried out or after the business partnership terminates:

a) Copies of documents or other technological support as proof of compliance of identification and Due Diligence obligation;
b) Sufficient Record of transactions to allow the reconstitution of each operation, in order to supply proof if necessary, within the scope of a criminal process;
c) Copy of all the commercial correspondence exchanged with the customer;
d) Copy of communication made by the relevant entities to the Financial Information Unit and other relevant authorities.

The internal Norm PCS.ARQ.01 – Central Archive explains in detail the procedures associated to the archive of information associated to the process of generation of business of the Banks.

7. Transaction Monitoring

Any operation that raises suspicion of being linked to Money Laundering, Funding of Terrorism and Proliferation of Weapons of Mass Destruction, must be examined carefully, independent of the amount involved. Norm MNA.OBS.220 – Potentially Suspicious Operations for Money Laundering shows common examples of suspicious Money Laundering operations.

If the review carried out concludes that there are reasonable signs or certainty that there is a link between the operation and the practice of Money Laundering, Funding of Terrorism and Proliferation of Arms of Mass Destruction, the operation in question must be reported immediately to competent authorities.

Generically, the operations are subject to: (i) general control carried out by any employee of the Bank who detected the operation; (ii) previous control carried out by the Compliance Directorate before the respective execution; (iii) Later control carried out by the Compliance Directorate after the execution of the operation.

The Bank, through the daily and automatic analysis of computer system data, executes the control of operations that imply alterations of entitlement of values, namely:

a) Cash operations, equal or above USD 15 000 or equivalent in Kwanzas;
b) Transfer from and to countries under counter measures or sanctioned;
c) Transfers equal or above USD 15 000 or equivalent in Kwanzas, destined for an offshore country;
d) Transactions equal or above USD 15 000 or equivalent in Kwanzas, destined for a risk country;
e) Credits in a single day period with cumulative amount above USD 15 000 or equivalent in Kwanzas;
f) Credits in a 3 consecutive days period with cumulative amount above USD 15 000 or equivalent in Kwanzas;
g) Credits in a 10 consecutive days period with cumulative amount above USD 30 000 or equivalent in Kwanzas;
h) Debits in a single day period, with a cumulative amount above USD 15 000 or equivalent in Kwanzas;
i) Debits in a 3 consecutive days period, with a cumulative amount above USD 15 000 or equivalent in Kwanzas;
j) Debits in a 10 consecutive days period, with a cumulative amount above USD 30 000 or equivalent in Kwanzas;

k) Clients making more than 10 credit transactions in 6 consecutive days, with a maximum cumulative amount of USD 3 000 or equivalent in Kwanzas;
l) Clients making more than 15 credit transactions in 12 consecutive days, with a maximum cumulative amount of USD 5 000 or equivalent in Kwanzas;
m) Clients making more than 10 debit transactions in 6 consecutive days, with a maximum cumulative amount of USD 3 000 or equivalent in Kwanzas;
n) Clients making more than 15 debit transactions in 12 consecutive days, with a maximum cumulative amount of USD 5 000 or equivalent in Kwanzas;

The Bank will adopt measures to determine the profile of each Customer in the operations execution in order to identify situations of embezzlement that should be more carefully analyzed.

When the nature or volume of Customers active or passive operations do not correspond to its activity or operational history, the Customer Bank Advisor must detect the occurrence and communicate a significant alteration in the Customer operation to the Compliance Directorate.

The Bank will pay special attention to situations where the same account, without apparent justification, has been credit through deposits in cash by many different people.

In any case, the Bank may put in place any other type of tool or control for the detection of operations prone to be seen as suspicious.

Every month, the Compliance Officer is responsible for presenting to the Chief Financial Officer a report with the main activities developed within the scope of prevention of Money Laundering, Funding of Terrorism and Proliferation of Weapons of Mass Destruction and corresponding detected cases.

8. Reporting of Suspicious Transactions

Any operation considered suspicious showing signs of being linked to the practice of Money Laundering or Funding of Terrorism, as well as any later circunstance related with these operations, must be reported immediately to the Compliance Officer.

- **Reporting Procedures**

The Bank employee that detects a suspicious operation of Money Laundering or Funding of Terrorism and Proliferation of Weapons of Mass Destruction must report it simultaneously to the his Senior and to Compliance Officer that, after careful review of the operation, will decide to report it to the Financial Information Unit.

9. Freezing of Funds

The Bank must freeze, without previous notice, all funds/economic resources belonging to or detained direct/indirectly, in the following detected cases:

- Customers linked to countries, entities or sanctioned individuals, *as per* Angolan Legislation and UN Security Council Resolution or other internationally accepted body,
- Fake Banks; and
- Anonymous entities or controlled by anonymous individuals.

10. Disclaimer

In accordance with Law 05/2020, good faith reporting made are not a violation of confidentiality, and does not imply responsibility for the reporter.

11. Confidentiality

The nature of communication and the identity of the employee that first reported the information are kept in strict confidentiality.

It is not allowed and it is a violation of the legal duty to inform the Customer or third parties the fact that an investigation or operation is under way, given the likelihood of connection with Money Laundering, Funding of Terrorism and Proliferation of Weapons of Mass Destruction except to people or specific internal entities and other competent authorities.

The non-compliance of the obligation of confidentiality is an offence punished with a fine in the amount of USD 25 000 and up to USD 2 500 000, if the agent is a company, or a fine in the amount of USD 12 500 to USD 1 250 000, if the agent is an individual.

The revelation or disclosure of the identity of the person who disclosed the information leading to the investigation of a specific operation is punished with a prison sentence of up to 3 years or a fine.

12. Training and Awareness of Employees

All employees of the bank will be entitled to Training namely specific training on the prevention of Money Laundering, Funding of Terrorism and Proliferation of Weapons of Mass Destruction. Periodic training sessions in person or E-learning will take place at the discretion of the Compliance Officer.

Alert emails to raise awareness on how to tackle some of the material on Money Laundering, Funding of Terrorism and Proliferation of Weapons of Mass Destruction will be sent.

Depending on the demand, the Compliance Officer and the Directorate of Organization and Quality (DOQ) may develop training tools and answer to questions on the topic of prevention of Money Laundering, Funding of Terrorism and the measures adopted by the Bank, with Bank employees being notified by email of any changes to current Policy or other relevant document related to it.