# POLICY FOR ANTI-MONEY AND COUNTER-TERRORISM FINANCING

April 2026

ATLANTICO EUROPA

# Table of Contents

## Framework

Banco Atlântico Europa - Namibia Branch ("Bank") assumes as its fundamental principle the active prevention of money laundering and terrorist financing ("ML/CFT") by adopting practices implemented in the Portuguese and Namibian market following the laws and regulations in force national and international, as well as with all good recognised practices.

The Bank adopts a policy of collaboration with the relevant ML/CFT competent authorities.

To comply with the legal and regulatory rules to which it is subject, the Bank adopts internal rules and procedures that enable it to know its Customers and the activities they carry out, as well as those that enable them to carry out their banking and financial activities in accord with deontological rules.

The current Policy applies to all Bank Employees and may extend to branches, subsidiaries and representative offices of the Bank and their employees to the extent approved by their respective bodies and, whenever necessary, it is adapted to the local law, legislation and regulation.

## Regulation

The rules and procedures contained in this Policy are mandatory in nature and must be fully observed by the Bank's employees at all times, as well as by its external employees, advisors and third parties acting on behalf of the Bank.

This Policy is designed to promote compliance with current legal and regulatory provisions and internal rules furthermore established by the Bank in preventing money laundering and combatting terrorist financing ("ML/CFT") and every employee that receives the document is obliged to consult the current legal norms or guidelines to which it refers.

## International Domain

a) 40 FATF recommendations, revised in 2017 (incorporating 9 recommendations on combatting terrorist financing);
b) (EU) Regulation 2015/847 of the European Parliament of 20 May (on information accompanying transfers of funds);
c) (EC) Regulation No 881/2002, as amended by the Council Implementing Regulation (EU) 2017/1834 of the Commission dated 9th October (establishing counter-terrorism measures directed against certain persons and entities);
d) (EC) Regulation No 2580/2001, as amended by the Council Implementing (EU) Regulation 2017/965 of 8th June (laying down measures against certain persons and entities).
e) 40 FATF recommendations, revised in 2017 (incorporating 9 recommendations on combatting terrorist financing);
f) (EU) Regulation 2015/847 of the European Parliament of 20 May (on information accompanying transfers of funds);

g) (EC) Regulation No 881/2002, as amended by the Council Implementing Regulation (EU) 2017/1834 of the Commission dated 9th October (establishing counter-terrorism measures directed against certain persons and entities);
h) (EC) Regulation No 2580/2001, as amended by the Council Implementing (EU) Regulation 2017/965 of 8th June (laying down measures against certain persons and entities);

## In the Portuguese domain

a) Law no. 83/2017 dated 18 August (on the prevention of money laundering and terrorist financing);
b) Law no. 52/2003, dated 22 August (approves the counter-terrorism);
c) Law no. 89/2017 dated August 21 (on the Permanent Beneficiary's Central Registry);
d) Ordinance no. 292/2011 of November 8, as amended by Ordinance no. 345-A / 2016 of December 30 (which approved the list of countries, territories, and regions with clearly more favourable privileged tax regimes);
e) Bank of Portugal Notice no. 1/2022 (on operating conditions, procedures, instruments, mechanisms, formalities for implementation, reporting obligations and other aspects necessary to ensure compliance with the preventive duties of money laundering and terrorist financing, within the scope of the activity of financial entities subject to the supervision of the Bank of Portugal);
f) Instruction no. 5/2019 (on information requirements on money laundering risk management and terrorist financing to be reported to Bank of Portugal);
g) Bank of Portugal Circular Letter no. 91/2006 / DSB (on non-cooperating countries and territories);
h) Law no. 83/2017 dated 18 August (on the prevention of money laundering and terrorist financing);
i) Law no. 52/2003, dated 22 August (approves the counter-terrorism);
j) Law no. 89/2017 dated August 21 (on the Permanent Beneficiary's Central Registry);
k) Ordinance no. 292/2011 of November 8, as amended by Ordinance no. 345-A / 2016 of December 30 (which approved the list of countries, territories, and regions with clearly more favourable privileged tax regimes);
l) Bank of Portugal Notice no. 1/2022 (on operating conditions, procedures, instruments, mechanisms, formalities for implementation, reporting obligations and other aspects necessary to ensure compliance with the preventive duties of money laundering and terrorist financing, within the scope of the activity of financial entities subject to the supervision of the Bank of Portugal);
m) Instruction no. 5/2019 (on information requirements on money laundering risk management and terrorist financing to be reported to Bank of Portugal);
n) Bank of Portugal Circular Letter no. 91/2006 / DSB (on non-cooperating countries and territories).

## In the Namibian domain

a) Financial Intelligence Act 2007 Repealed (on the prevention of money laundering and terrorist financing);
b) Financial Intelligence Act 13 of 2012;
c) Directive 02 of 2017 on Availing Records and Information;
d) Directive 01 of 2022 on Effectiveness of Sanctions Screening Systems;
e) Directive (Legal Practitioners) No 02 of 2016, Directive to Legal Practitioners on Mandatory cash Transactions Reporting;
f) (Revised) Directive 01 of 2016 on Strengthen Controls on Cross Border Remittances;
g) General Compliance Circular 01 of 2023 (High Risk and Non-Cooperative Jurisdictions);
h) Guidance Note no. 01 of 2015 on Beneficial Ownership Identification;

i) Guidance Note no. 01 of 2017 on De-Risking;
j) Guidance Note no. 01 of 2023 (customer due diligence, detections and reporting of suspicions ADLAs/Money Services Businesses);
k) Guidance Note 13 of 2023 – Implementing Risk Based Controls NPO (Non-profit organisations: all charities and religious or faith based organisations);
l) General Compliance Circular 01 of 2021 Final Release of NRA Report;
m) Prevention and Combating of Terrorist and Proliferation Activities Act no 04 of 2014;
n) General Compliance Circular 1 of 2023;
o) General Compliance Circular 02 of 2023 June;
p) General Compliance Circular 03 of 2023 October;
q) Guidance Note 11 of 2023 – Risk Based Approach for VASPs 2023;
r) Guidance Note 10 of 2023 – Risk Assessment for VASPs;
s) Guidance Note 12 of 2023 Understanding Risks and TF Indicators NPO;
t) Guidance Note 13 of 2023 Implementation Risk Based Controls NPOs;
u) Directive 01 of 2024 on UBO Information;
v) Directive 02 of 2024 on NPO Risk Assessment
w) Directive 01 of 2023 Implementation of Mandatory Beneficial Ownership (BO) Information Forms with the Business and Intellectual Property Authority (BIPA)

## In the European Domains

a) ECB SSM Supervisory Statement on Governance and Risk Appetit;
b) Delegated Regulation (EU) 2019/758 of the Commission, of January 31, 2019, which complements Directive (EU) 2015/849 of the European Parliament and of the Council, regarding to technical standards regulating minimum measures and the type of additional measures that credit and financial institutions must take to mitigate the risk of money laundering and terrorist financing in certain third countries;
c) Regulation (EU) 2018/1672 of the European Parliament and of the Council, of 23 October 2018, on the control of sums of cash entering or leaving the European Union;
d) Delegated Regulation (EU) 2016/1675 of the Commission, of 14 July 2016, which completes Directive (EU) 2015/849 of the European Parliament and of the Council, identifying high-risk third countries with strategic weaknesses;
e) Regulation (EU) 2015/847 of the European Parliament and of the Council, of 20 May 2015, concerning the information on the payer that must accompany the transfer of funds;

## Concepts

Money Laundering means any activity meant to: engages, directly or indirectly, in transactions that involve proceeds of any unlawful activity; acquire, possess or use or remove from or bring into Namibia proceeds of any unlawful activity or conceal, disguise or impede the establishment of the true nature, origin, locations, movement, disposition, the title of rights with respect to, or ownership of, proceeds of any unlawful activity.

Advantages mean goods derived from the practice of co-funding of typical illegal acts of pimping, sexual abuse of children or dependent minors, extortion, drug and psychotropic substances trafficking, arms trafficking, organ or human tissue trafficking, trafficking of protected species, tax fraud, influence peddling, corruption and other offences referred to in measures to combat organised and economic

and financial crime, and typical unlawful acts punishable by imprisonment of at least 6 months or a maximum duration of more than 5 years, as well as the goods obtained therein.

Terrorism activity means any concerted action aimed at undermining national integrity and independence, preventing, altering or subverting the functioning of state institutions provided for in the Constitution, forcing the public authority to execute an act, or to refrain from it or tolerate it, or to intimidate certain persons, groups of people or the general population by perpetrating:

a. Crime against the life, physical integrity or freedom of individuals;
b. Crime against the security of transport and communications, including computer, telegraph, telephone, radio or television;
c. Crime of a deceitful spread of common danger through fire, explosion, release of radioactive substances or toxic or choking gases, flood or avalanche, building collapse, contamination of food and water intended for human consumption or spread of disease, pest, harmful plant or animal;
d. Acts that destroy or make it impossible to function or deviate from their normal purposes, the means or channels of communication, public service facilities or those intended to supply and meet vital needs of the population, whether permanently or temporarily, wholly or partially;
e. Research and development of biological or chemical weapons;
f. Crimes involving the use of nuclear energy, firearms, biological or chemical weapons, explosive substances or devices, incendiary means of any kind, parcel or mail bombs, which due to their nature or context are likely to seriously affect the state or population they intend to intimidate.

Beneficial Owner is any natural person on whose behalf a transaction or activity is carried out, who ultimately owns the property, or has legal control over the Customer.

Beneficial Owner of Corporate Entities in cases where the Customer is a corporate entity with no shares allowed for trading on a regulated market (or is subject to disclosure requirements equivalent to those required by European Union law and applicable law), the following Beneficiaries are deemed Beneficial Owners:

a. The natural person or persons who ultimately own or directly control an adequate percentage of shares, voting rights or equity interest of a legal person. For these purposes, direct ownership is said to exist where a natural person detains holdings representing more than 20% of the Customer's share capital;
b. The natural person or persons who ultimately own or indirectly control an adequate percentage of a legal person's shares or voting rights or equity holdings. For these purposes, indirect ownership is represented by capital holdings representing more than 20% of the customer's capital stock by:
    - A corporate entity controlled by one or more natural persons; or
    - Several corporate entities controlled by the same natural person or persons.
c. The natural person or persons who exercise control by other means over that legal person;
d. The natural person or persons holding top management if, after exhausting all possible means and provided there is no reason for suspicion:
e. No person has been identified under the preceding subparagraphs; or
f. Doubts prevail that the person or persons identified are the beneficial owners.

Beneficial Trust Owner and other non-corporate legal persons when the Customer is a trust or another non-corporate legal person, the Beneficial Owners are:

a. The founder (settlor in the case of trusts);
b. The trustees of trusts, or their trustees in the case of other non-corporate legal persons;
c. The trustee, if applicable;
d. Beneficiaries or, if they have not yet been determined, the category of persons in whose primary interest the trust or non-corporate legal person has been incorporated or is active;
e. Any other natural person who has ultimate control of the trust or non-corporate legal person through direct or indirect holdings or other means.

Politically exposed persons 'PEP' natural persons who perform or have performed the following prominent higher-level public functions in any country or jurisdiction for the past year:

a. Heads of State, Heads of Government and members of Government, namely ministers, secretaries and undersecretaries of state or those holding an equivalent status.
b. Members of Parliament or other members of parliamentary chambers;
c. Judges of the Constitutional Court, Supreme Court of Justice, Supreme Administrative Court, Court of Auditors, and members of supreme courts, constitutional courts and other high-level judicial bodies of other states and international organisations;
d. Representatives of the Republic and members of the governing bodies of the autonomous regions;
e. Ombudsman, State Councillors, and members of the National Data Protection Commission, the Higher Council of the Judiciary, the Higher Council of the Administrative and Fiscal Courts, the Attorney General's Office, the Higher Council of the Public Prosecution Service, the Higher Council of National Defence, the Economic and Social Council, and the Media Regulatory Authority;
f. Heads of diplomatic missions and consular posts;
g. Armed Forces General Officers in Permanent Service and Republican National Guard Officers, as well as Public Security Police Superintendent-Chiefs;
h. Presidents and councillors with executive functions in city councils;
i. Members of central banks' management and supervisory bodies including the European Central Bank;
j. Members of the administrative and supervisory bodies of public institutes, public foundations, public establishments and independent administrative entities, whatever their designation;
k. Members of management and supervisory bodies of entities belonging to the public business sector, including the business, regional and local sectors;
l. Members of the executive governing bodies of national or regional political parties;
m. Directors, deputy directors and members of the board of directors or persons performing equivalent duties in an international organisation[1].

Occasional transaction is any transaction made by the obliged entities outside the scope of an already established business relationship, characterised in particular by its occasional nature.
Unacceptable customers unidentified Customers or numbered accounts, nor does it accept account openings which present signs of fraud. Additionally, the following cases are considered unacceptable ML / TF risk Customers:

[1] All the other information relating the association to PEP is describe on the Account Opening Manual.

a) Customers related to countries, entities or individuals sanctioned by the UN and the European Union, among other entities;
b) Customers who present suspicious behaviour or odd questioning;
c) Customers and/or related entities (in case of legal persons: representatives, capital holders, beneficial owners/top-level management, administrators) referenced on ML/FT databases;
d) Previous reports of attempted fraud or other risk behaviour on the Customer's history;
e) Customers or entities who were previous customers and had their accounts closed due to compliance reasons;
f) Shell banks;
g) Anonymous entities, or entities controlled by anonymous individuals;
h) Lack of information about the nature and purpose of the business and the origin and destination of customer funds;
i) Customers using their accounts with the Bank for virtual assets trading activities.

Any exceptions to the cases presented above must be previously submitted to the Compliance Department for consideration and subject to approval by the Bank's Executive Committee.

Freeze means the prohibition of the use, transfers, conversion, disposition or movement of any funds, economic resources, property or other assets that are owned or controlled by designated persons or entities.

## Duties

The Bank is required to fulfil the following duties:

Availing Records means providing information to re regulator (FIC/NAMFISA) in time when records and information are requested, same should be availed within the most reasonable time such reasonable time should not exceed three days, however when not possible to achieve the time requested the Bank should communicate with the regulator.

### Identification and due diligence duty

The Bank must identify Customers, natural or legal persons, whether they are holders or representatives, and the verification must be done by submitting original supporting documents in accordance with legislation. All account opening processes and supporting documents will be archived in the systems established for this purpose.
The Bank also must identify the parties when conducting an occasional transaction.

### Complementary due diligence procedures

The bank should further adopt procedures complementary enhanced due diligence procedures in addition to regular ones depending on the level of risk of each customer.

### Duty of refusal

The Bank shall refuse to initiate business relationships, conduct occasional transactions or perform other transactions when it:

a. Does not obtain the personal documentation/identifying data and the respective means of proof regarding the Customer, it is representative and/or Beneficiary;
b. Does not obtain the information necessary for assessing the integrity of the Beneficial Owner and the ownership and control structure of the Customer;
c. Does not obtain information on the nature, object and purpose of the business relationship;
d. Does not manage to perform the necessary procedures to comply with the duty of updating information.

The Bank shall include in a document or written record, the possible reasons for the impossibility of complying with the due procedures, as well as the grounds for any termination of business relationships already established, and also refer to any consultations with the authorities, indicating their dates and the means of communication used.

### Record register duty

The Bank shall keep records of proof of identification, as well as any other transaction record documents enabling their tracking, under Law No. 83/2017, article 51.º, for a period of 7 (seven) years from the date of execution, even if the business relationship has already ended.

The Bank shall keep copies of all communications made under the reporting obligation for a period of 7 (seven) years from the time each communication is made.

Under the Act 23 of 2012 section 27 the records should be kept for a period of 5 (five) years since Portuguese law is more extensive the Branch is following the 7 (seven) year's period instead of 5 (five) which is obligatory in Namibia.

Notwithstanding the preceding paragraphs, the Bank shall, in any event, take all necessary measures in responding fully to requests from the authorities to determine whether they still maintain or maintained for the past 10 years, business relationships with a given natural, legal or similar person, and describe the nature of those relationships.

### Analysis duty

The Bank should pay particular attention to transactions which by their nature, complexity, purpose, unusual character in the Customer's manner of operation, amounts involved, frequency, the economic and financial situation of the intervening Customers or the means of payment used and the profile of the interveners are likely to be related to money laundering or terrorist financing.
For purposes of the preceding article, the Bank shall, in particular, consider the following characteristics:

a. Nature, purpose, frequency, complexity, unusualness and atypicality of conduct, activity or operations;
b. Apparent absence of an economic objective or a lawful purpose associated with conduct, activity or operations;
c. Amounts, origin and destination of the funds moved;
d. Place of origin and destination of the operations;
e. Means of payment used;
f. Nature, activity, operating pattern, economic and financial situation and the profile of the interveners;
g. Type of transaction, product, corporate structure or centre of interest without legal personality that may favour anonymity.

### Communication duty

The Bank shall immediately inform the Financial Intelligence Centre (FIC) whenever it has knowledge of, suspects or has good reason to suspect that certain funds or other assets, regardless of the amount involved, originate from criminal activities or are related to the financing of terrorism.

The Bank shall also report, on a systematic basis, to the FIC and Bank of Namibia, any types of operations that may be defined by specific regulations.

The form, term, content and other terms of the systematic statements issued by the Bank and the Branch shall be following the applicable legislation.

### Abstention and suspension of decisions duty

The Bank should refrain from performing operations that it knows or suspects are related to money laundering or terrorist financing crime.
The Bank shall immediately discharge its obligation to notify (effected by the above regarding communication duty) when it refrains from executing any transaction, informing the authorities of the reason for the abstention.
The Bank reports all suspicious activities and transactions under the Act 13 of 2012 section 33:

a. Suspicious transactions or activities that are submitted on GO AML and retain the record for the period mentioned in the Record Register duty.
b. The Bank ensures that without a response from the regulator, the final decision relating to the transaction has the conclusion from de Head of Compliance or MRLO.

If the Bank considers that abstaining from the execution of the operation is not possible, or if, after consulting the Attorney General of the Republic and the Financial Intelligence Unit, it is found that it may hinder the investigation and prosecution of the beneficiaries of the operation, it may be carried out and the bank should immediately provide to the judicial system with information about it and this documentation shall be kept on record for a minimum of 7 years and permanently made available to the sectoral authorities.
If notified of the judicial system decision to temporarily suspend the operation, the Bank shall suspend that operation until it is subject to judicial review, which shall determine whether or not to maintain the temporary suspension of the operation.

### Collaboration duty

The Bank shall provide all assistance required from the regulator and other competent judicial and police authorities or competent authorities to supervise compliance with legally established duties.

### Non-disclosure duty

The Bank, members of its governing bodies, persons performing board, management or leadership functions, as well as their employees, proxies and other persons providing services to them, may not disclose to the Customer or third parties that a criminal investigation is in course or that legally due information about an operation was disclosed.
The Bank assures that eventual and necessary contacts established with Customers involved in the communications which derive from investigations or ongoing criminal proceedings are processed, whenever adequate, in articulation with the Regulatory Compliance Officer and, whenever necessary, with the judicial authorities or competent police.

### Control duty

The Bank shall adopt internal control, risk assessment and management, internal audit and reporting policies and procedures that enable it to comply with the legal duties to which it is subject and to be able to prevent operations related to money laundering and terrorism financing.

### Training duty

The Bank shall implement training mechanisms so that all its managers and employees are aware of the obligations to which the Bank is subject in the prevention of money laundering and terrorist financing and are able to recognise operations that may be related to this type of illegalities.
The Bank shall ensure that the persons referred to in the preceding paragraph are provided specific and regular appropriate training for each sector of activity enabling them to recognise operations that may be related to money laundering and terrorist financing.
In the case of new hires whose duties are directly relevant to the prevention of money laundering and terrorist financing, the Bank shall provide them with adequate training, immediately after their admission, in the policies, procedures and controls internally defined for the purpose.
Training shall be provided by persons or entities with recognised competence and experience in the prevention and combatting of money laundering and terrorist financing.
The Bank will keep an up-to-date and complete record of the training carried out for 7 years from completion and make it permanently available to the sectoral authorities.

## Data protection and processing

The Bank is authorised to carry out the processing of personal data required in executing legally prescribed duties.
The Bank's processing of personal data is solely to prevent money laundering and terrorist financing and may not be processed for any other purpose, including commercial purposes, without prejudice to other laws applicable to the processing of personal data.
The Bank ensures the elimination of personal data as soon as the retention periods associated with the document record maintenance obligation have expired.

## Specific obligations

As a financial entity, the Bank is especially required to comply with the following:

a. The opening, maintenance or existence of anonymous accounts, as well as the use of fictitious names or titles are not permitted;
b. Enhanced due diligence measures should be applied to cross-border correspondence relations with institutions based in third countries, obtaining information on the nature of their business, internal control procedures in the area of money laundering and terrorist financing and the characteristics of their supervision;
c. When establishing correspondence relationships involving institutions based in third countries, the Bank shall put down in writing the respective responsibilities of each institution;
d. Correspondence relations with shell banks is prohibited.

## Administrative Offence

Without prejudice to criminal liability for the crime of money laundering to which both natural and legal persons may be subject or other related sanctions applicable to each in this case, administrative offences are defined as non-compliance with the duties and obligations imposed by the regulation, for which they may be liable:

a) Financial entities;
b) Non-financial obliged entities:
c) Individuals who hold positions of administration, management, governance, leadership or supervision, representatives, workers or other employees, whether permanent or occasional.

Liability of the legal or similar person is excluded only when the agent acts against express orders or instructions from that person.

Non-compliance with the duties and obligations imposed by the Prevention and Combating of Terrorist and Proliferation Activities Act 4 of 2014 is punishable as an administrative offence.

## Offence of terrorism and funding of terrorist activities

A person who, in or outside Namibia, directly or indirectly engages in any proliferation activity commits the offence of proliferation and is liable to life imprisonment.
A person who by any means, in or outside Namibia, directly or indirectly, provides financial services or solicits or collects funds intending, knowing or having reasonable grounds to believe that such funds are to be used in whole or part, to carry out any proliferation activity, regardless of whether such funds or part thereof were actually used to commit a proliferation activity, commits an offence and is liable to a fine not exceeding N$100 million or to imprisonment for a period not exceeding 30 years, or to both such fine and such imprisonment.

## Offence of proliferation and funding of proliferation activities

A person who, in or outside Namibia, directly or indirectly engages in any proliferation activity commits the offence of proliferation and is liable to life imprisonment.

A person who by any means, in or outside Namibia, directly or indirectly, provides financial services or solicits or collects funds intending, knowing or having reasonable grounds to believe that such funds is to be used in whole or part, to carry out any proliferation activity, regardless of whether such funds or part thereof were actually used to commit a proliferation activity, commits an offence and is liable to a fine not exceeding N$100 million or to imprisonment for a period not exceeding 30 years, or to both such fine and such imprisonment.

## Offences associated or connected with funding of specified offences

A person who intentionally, directly or indirectly, in whole or in part, and by any means or method:

- Deals with, enters into or facilitates any transaction, or enables the acquisition of a business interest, or performs any other act in connection with funds, which such person knows or ought reasonably to have known or suspected to have been acquired, owned collected, used, possessed, owned or provided for the:
    i) commission or facilitation of a specified offence;
    ii) benefit of, or on behalf of, or at the direction of, or under the control of a person that commits or attempts to commit or facilitates the commission of a specified offence;
    iii) benefit of a designated person, organisation or country;
    iv) benefit of a designated country where reasonable grounds exists to suspect a violation of the Security Council sanction;
    v) benefit of a proscribed person or organisation.

- Provides financial or other services in respect of funds, acquisition of a business interest, commits an offence and is liable to a fine not exceeding N$100 million or to imprisonment for a period not exceeding 30 years, or to both such fine and such imprisonment.

- A person who knows or ought reasonably to have known or suspected that funds or a business interest are being acquired, collected, used, possessed, owned or provided for purposes as contemplated underneath and enters into, or becomes concerned in an arrangement which in any way has or is likely to have the effect of:

    a) facilitating the retention, control or transfer of ownership of such funds by or on behalf of: person that commits or attempts to commit or facilitates the commission of a specified offence; or a designated or proscribed person or organisation;
    b) converting such funds;
    c) concealing or disguising the nature, source, location, disposition or movement of such funds, the ownership thereof or any interest a person may have therein;
    d) removing such funds from a jurisdiction; or transferring such funds to a nominee, commits an offence and is liable to a fine not exceeding N$100 million or to imprisonment for a period not exceeding 30 years, or to both such fine and such imprisonment.

## Policies and Internal Procedures

## 1. Organisation and Risk Management

Those responsible for the Bank's business and support areas are also responsible for:

a. Implementing, controlling and verifying the level of compliance with prevention and control procedures in its organisational unit, keeping the Compliance Department informed.
b. Knowing and monitoring the occurrences related to money laundering and terrorist financing verified in its organisational unit, keeping the Compliance Department informed.
c. Suggesting and implementing, in collaboration with the Compliance Department, any additional control procedures and precautionary measures it deems necessary, based on the specificities of its organisational unit, to detect and prevent suspicious operations.

The Bank's Board of Directors is responsible for the implementation and enforcement of policies and procedures and controls in the prevention of money laundering and terrorist financing, in particular with the following responsibilities:

a. Approving the policies and procedures and internal controls appropriate to the Bank's activity, as well as updating them, being responsible, in particular for the annual review and updating of this Policy;
b. Having adequate knowledge of the money laundering and terrorist financing risks to which the Bank is exposed, as well as the processes used to identify, assess, monitor and control such risks;
c. Ensuring that the Bank's organisational structure at all times allows for the proper implementation of appropriate policies and procedures and controls, preventing conflicts of interest and, whenever necessary, promoting the separation of roles within the organisation;
d. Promoting a culture of anti-money laundering and terrorist financing that encompasses all Bank employees whose roles are relevant for the purpose of preventing money laundering and

terrorist financing, sustained by high standards of ethics and integrity, and, whenever necessary, in defining and approving appropriate codes of conduct;

e. Appointing the Regulatory Compliance Officer;
f. Monitoring the activity of other members of senior management as they protect business areas that are or may be exposed to money laundering and terrorist financing risks;
g. Periodically monitoring and evaluating the effectiveness of policies and procedures and controls approved and implemented, ensuring the implementation of appropriate measures to correct the deficiencies found in them.

## The Regulatory Compliance Officer shall:

a. Perform their duties independently, permanently, effectively and with the decision-making autonomy necessary for such exercise, whatever the nature of their relationship with the Bank;
b. Have the aptitude, professional qualification and availability appropriate to the exercise of the function;
c. Have adequate technical, material and human resources, including those necessary for the proper performance of the function;
d. Have unrestricted and timely access to all internal information relevant to the exercise of the function, in particular, information regarding the execution of the identification and due diligence duty and the records of the operations performed;
e. Not be subject to potential functional conflicts, especially when there is no segregation of its functions.

The Bank shall also designate a member of the management body responsible for controlling the ML/FT regulatory compliance, ensuring that this member:

a. Has the necessary knowledge for the comprehension of the subjects that the position entails;
b. Performs their duties with a sense of availability, decision-making autonomy and the necessary resources for their performance;
c. Has full and timely access to all information and internal documentation relevant to the performance of their duties;
d. Performs those duties with an adequate segregation of potentially conflicting duties, assuring that any potential situations of conflict of interests are timely identified, minimized and subjected to careful and independent monitoring.

The Internal Audit Department is responsible for regularly monitoring and testing the design, efficiency and effectiveness of the Bank's ML/CFT program, thereby also providing additional assurance to the Board of Directors in these matters.

## The Head of the Internal Audit Department is responsible for:

a. Monitoring the performance of the functional areas and the Compliance Department; and,
b. Performing design and effectiveness tests on ML/CFT controls;
c. To this end the Bank shall:
d. Continuously evaluate the applicability of the procedures in force;
e. Define and monitor the main risks and related indicators associated with ML/TF;
f. Ensure an effective training strategy; and,
g. Periodically perform effectiveness tests on the procedures and systems adopted.

In addition, in order to gain a deeper and more independent view of the effectiveness and efficiency of the ML/CFT Program, the Bank should also regularly conduct specialised external audits on these matters.

The Compliance Department, periodically and independently, carries out prior and /or post-monitoring of the quality, adequacy and effectiveness of the anti-money laundering and counter-terrorism policies, procedures and control systems in force. This control is carried out in parallel with the work performed by the internal audit department and the external auditors.

The Bank's Board of Directors together with the Compliance Department identifies the concrete risks of money laundering and terrorist financing in the Bank's specific operating reality including associated risks according to:

a. The nature, size and complexity of the Bank's activity;
b. Their Customers;
c. Business areas developed, as well as the products, services and operations made available by the Bank, with particular attention to the risks that may arise from the offer of products or operations that may favour anonymity;
d. New business practices, distribution mechanisms or payment methods, as well as the use of new technologies in new or pre-existing products;
e. Distribution channels for the products and services available, as well as the means of communication used in contact with Customers;
f. Countries or territories of origin of the obliged entity's Customers, or in which they are located or otherwise operating;
g. Countries or territories in which the obliged entity operates, directly or through third parties, whether or not belonging to the same group;

The Bank will take into account the likelihood and impact of each of the risks identified, and the overall risk of the Bank and its business areas.

For the purposes of compliance with the preceding paragraph, the Bank's Board of Directors will meet with the Compliance Department to assess the continuing adequacy of procedures to mitigate the concrete money laundering and terrorist financing risks to which the Bank is subject and, whenever applicable, it proposes and approves amendments to internal rules on money laundering and terrorist financing.

The Head of the Compliance Department makes available to the Bank's Board of Directors and Executive Committee a quarterly report on its activity including the work and controls carried out during the reporting period on the identified money laundering and terrorist financing risks, the effectiveness procedures and, where applicable, they suggest appropriate additional mechanisms to mitigate new risks that are identified.

The Bank's Board of Directors will provide the Compliance Department with adequate material and human resources to enable it to be adequately equipped to perform its functions in a timely, informed and independent manner.

Bank Employees play a crucial role in matters relating to ML/CFT. As such, all Bank Employees are responsible for ensuring that they comply with the provisions of this Policy.

In performing their daily duties, Employees must:

a. Remain vigilant to the possibility of ML / TF situations occurring;
b. Report immediately to the Compliance Department any suspicion of ML/TF;
c. Comply with all procedures related to Customer identification, account opening and maintenance, account monitoring, documentation maintenance and registration, and collaboration in providing information to the Compliance Department; and,
d. Ensure Customers are not notified of any reporting to authorities about their transactions.

Employees are also responsible for completing all ML/CFT trainings assigned to them and subsequently diligently applying the knowledge acquired in those trainings in accordance with their respective roles/responsibilities.

## 2. Employee Training

All Bank employees who are directly or indirectly involved in the prevention of money laundering and terrorist financing will be provided specific training in this area supervised by the Compliance Department. The training sessions are held with a maximum limit of 2 years and whenever there is a new regulation that justifies it.

In the case of new hires, employees whose duties are directly relevant to the prevention of money laundering and terrorist financing, after their admission and for up to 6 months the Bank provides them with appropriate training regarding policies, internal procedures and controls related to the prevention of money laundering and the financing of terrorism.

To the extent necessary, the Compliance Department and the Legal Department may develop training and clarification tools on the topic of prevention of money laundering and terrorist financing and implemented measures Bank staff must be notified via the Bank's Intranet platform of any change to this Policy.

At the end of each training, trainees must be evaluated to certify the acquired knowledge.

The Bank ensures that the training duty is performed at the same level and extent in what regards its branches and subsidiaries, including when applicable the abidance to the local laws and rules.

## 3. Control Mechanisms

The Bank adopts internal control mechanisms and procedures in the assessment and management of the ML/TF risk, complemented by a communication system (internal and for legal authorities) to mitigate or prevent this risk. For control purposes, the Bank shall continually ensure the applicability of existing procedures by defining and monitoring the main ML/TF indicators and risks.

### ML/TF Risk assessment

The Bank is responsible for adopting internal control, risk assessment and management, internal audit and reporting mechanisms and procedures that enable it to comply with the legal duties to which it is subject, and which are capable of preventing transactions related to ML/TF.

The Bank adopts internal control mechanisms and procedures in the assessment and management of risk compliance in ML/CFT, complemented by a communication system (internal and for legal

authorities) to mitigate or prevent this risk. The process design includes primary activities intended to execute operations, identify and accept its stakeholders, as well as the control activities performed by deployment units, the Compliance Department and the Internal Audit Department.

Other factors which show fit to the Bank's operational reality should also be considered since the isolated presence of factors and indicative types of risk does not necessarily determine the automatic attribution of high or low risk to a certain business relationship or occasional transaction.

For this purpose, the Bank defines its controls based on an annual assessment of its exposure to ML/TF risk. The risk assessment methodology is based on the following risk factors identified by the Bank:

a. Characteristics of the customer base;
b. Distribution channels for goods and services;
c. Country of residence and nationality of Customers;
d. Customer activity sectors; and,
e. Business segments.

The Bank's risk is mitigated by the ML/CFT internal control system. The Compliance Department is responsible for performing the risk assessment. If the assessment identifies certain risks which are not being properly mitigated, the Compliance Department should propose an action plan to implement new controls and/or revise existing ones.
The decision to manually review the types of risk which are automatically attributed must always be well grounded. This decision is up to the Regulatory Compliance Officer or any other employee of the Bank who is not directly involved in the commercial relationship with the Customer, under the supervision of the former.

The Bank must ensure that it has all relevant information about the persons and entities with whom it relates. Accordingly, it shall ensure that it adopts a risk-based due diligence methodology. With this approach, counterparties with high ML/TF risks should be considered as high risk and due diligence and reinforced monitoring should be undertaken.
The Bank shall regularly update counterparty due diligence information during the business relationship to ensure accurate risk rating. Due diligence should be reviewed if an event indicates that the risk associated with the Customer has changed (e.g., blocked or even rejected transactions, or negative information from public sources of information). For Customers classified as high-risk, due diligence should be reviewed at least every two years.

## Screening

Screening plays a relevant role in identifying the risks associated with ML/TF. As such, the Bank shall implement controls that allow the screening of Customers and their relevant related parties (*e.g.* Beneficial Owners, subscribers, attorneys, among others), Transactions and Suppliers, in line with the provisions of this Policy and the Sanctions Policy.

The automatic screening systems used by the Bank must meet the minimum fuzzy matching requirements. This mechanism allows the setting of a match percentage, and only notifications indicating a higher level of similarity than the set value will be investigated, thus allowing the assignment of a probabilistic classification screened case-by-case. Screening systems shall be calibrated according to the Bank's risk assessment.

The Bank's screening systems take into account the latest current listings for PEPs and Sanctions entities.

Screening should be undertaken for:

a. All new Customers and their respective relevant related parties;
b. Bank Suppliers and Employees;
c. All existing Bank Customers ongoing;
d. When there are changes in counterparty information;
e. When new additions are made to the Sanctions and PEPs lists; and,
f. Transfers and payments issued/received from Customers targeting or originating from other banks.

For the purposes of this Policy, it is noted that in addition to the possible self-declaration of a Customer as a PEP, it is the screening system that acts as a PEP identification control for the subsequent enhanced due diligence process. In the same context, this is the system used to identify sanctioned parties with which the Bank cannot establish business relationships or, if these relationships existed prior to the Sanction, they should be frozen and reported to the Authorities.

At the beginning of the commercial relationship, the screening is carried out manually by the CD on the screening platform used, when carrying out the analysis of the account opening process.

The ongoing screening carried out for Bank Customers is carried out automatically by the system and whenever there is a match that is not immediately verified as a false positive, the CD analyzes and validates the hit in question. In this validation, if there are doubts about whether it effectively deals with the customer or not, the CD checks on internet sites if it can obtain additional information and, whenever necessary, poses additional questions to the business area, which must apply them to the customer.

The screening of operations is also carried out manually by the CD on the screening platform used, when carrying out the analysis of the operation.

## Customer risk classification

The Bank's and ML/CFT reputational defence processes framed in a logic of differentiation and grading of ML/TF risk, only become truly effective with the implementation of classification, analysis and monitoring policies that allow perception at all times of the risk level of the entity. Under these circumstances, all Bank Customers are classified as:

### High Risk (1)

The entities which fall into this category are:

- Entities classified as PEPs;
- Entities (including Beneficial Owners) referred in legal or tax proceedings due to ML/CFT Investigations;
- Entities residing in offshore jurisdictions or residing in high-risk countries;
- Legal persons whose CAE includes high-risk activities; and
- Entities who have been attributed this rating by the Regulatory Compliance Officer.

### Medium Risk (2)

The entities which fall into this category are:

- Entities residing or headquartered in medium-risk countries (excepting Namibia[2]);
- National Entities of offshore jurisdictions or of high-risk countries;

[2] Since the Branch is located in Namibia, ATLANTICO concluded that our Namibian clients would be considered low risk.

- Legal Entities whose CAE includes medium-risk activities; and
- Entities who have been attributed this rating by the Regulatory Compliance Officer.

**Low Risk (3)**

The entities which fall into this category are:

- Entities residing or headquartered in jurisdictions belonging to the European Union or similar countries;
- Nation Entities of medium-risk countries or jurisdictions belonging to the European Union or similar countries;
- Legal entities whose CAE includes low-risk activities and
- Entities who have been attributed this rating by the Regulatory Compliance Officer.

The level of risk attributed to each entity only has an influence on the risk which is attributed to the Customer, which means that the attributed risk might differ among the entities which belong to the same Customer. Only the entities rated as PEP imply the attribution of aggravated risk to all singular entities belonging to the same Customer.

During the business relationship established with Customers or guarantors, the Bank conducts periodic and non-periodical diligences and procedures to ensure the timeliness, accuracy and completeness of the information it already has. The data update period is directly associated with the customer risk level using the following criteria:

High Risk (1): Every year or after the expiry date;
Medium Risk (2): Every 3 years or after the expiry date; and,
Low Risk (3): Every 5 years or after the expiry date.

## 4. Customer Identification and knowledge

Considering that knowing the Customer is a key instrument in the fight against the use of the financial system for money laundering and terrorist financing, the Bank undertakes to solely enter into a business relationship with Customers who provide information required by law, after analysing this information.

The Bank has developed the account opening process to enable all information about the Customer and their Beneficiaries (if applicable) to be collected and recorded, prior to the commencement of business relationships with the Customer. All relevant identification data should always be verified through original supporting documents or certified copies of which the Bank must keep copies.

The Compliance Department may determine the need to collect additional information when the Customer engages in an activity deemed to be potentially risky based on Know Your Customer information.

The identification and due diligence procedures set out in this chapter regarding Customers and their representatives, as well as their Beneficial Owners shall be observed whenever the Bank:

a. Establishes business relationships (business or professional relationships expected to be of a lasting nature);
b. Undertakes occasional transactions of an amount of N$ 99.999,99 or more, either through a single transaction or through various transactions that appear to be related to each other;
c. Is aware that operations, regardless of their value and any exception or limit, may be related to money laundering or terrorist financing;

d. Has doubts about the accuracy or appropriateness of previously obtained customer identification data.

## Identification data

The following data shall be collected in identifying natural persons:

a. Photograph;
b. Full name;
c. Signature;
d. Date of birth;
e. Nationality on identification document;
f. Type, number, expiry date and issuing authority of the identification document;
g. Tax identification number or an equivalent issued by a competent foreign body;
h. Profession and employer identification (if applicable);
i. Full permanent address and, if different from the current address, the tax domicile;
j. Country of birth;
k. Other nationalities held which are not contained in the identification document.
l. In the case of Customer representatives, the Bank also verifies the document entitling them to act as representatives of the said Customer;
m. Financial information.

The following elements are collected in identifying legal persons or collective interest centres without a legal personality:

a. Name;
b. Object;
c. Full address of the registered head office and, where applicable, of the branch or permanent establishment or any other address of the main business locations;
d. Identification number of the legal person or equivalent issued by a competent foreign authority;
e. Identity of holders of equity interests and voting rights of 20% or more;
f. Identity of the members of the management body or equivalent, as well as other relevant senior staff with management powers;
g. Country of incorporation;
h. EA (Economic Activity) code, institutional sector code, or other similar code, if any;
i. Financial information.

## Supporting identification documents

Natural persons:
For the purpose of verifying the identity of natural persons, the Bank shall demand the presentation of a valid original identification document issued by a competent public authority containing a photograph, full name, signature, date of birth and nationality.

Legal persons and centres of collective interest without a legal personality ("similar entities"):
For the purpose of verifying the identification of legal persons, the Bank shall demand the legal entity´s identification card, the commercial registration certificate or, in the case of an entity with its registered office outside the national territory, an equivalent document issued by an independent and credible source, including the name, subject matter, full address of the registered office (and, where applicable, branch or permanent office) and the legal entity identification number (or equivalent, in the case of an entity with headquarters abroad).

## Identity Verification

Except in cases as set out below for situations where an identity check is exceptionally possible after the beginning of the relationship, the identity check is performed prior to the establishment of the business relationship or any occasional transaction.
Identity verification can only be completed after the business relationship has commenced, but as soon as possible, provided that the following assumptions are cumulatively met:

a. If it is necessary, not to interrupt the normal course of business;
b. The contrary is not the result of a legal or regulatory rule applicable to the Bank's activity;
c. The situation in question presents a low risk of money laundering and terrorist financing, expressly identified as such by the Bank;
d. The Bank shall implement appropriate measures to manage the risk associated with that situation, in particular by limiting the number, type or amount of transactions that may be carried out.

## Due diligence procedures complementary to identification

According to the risk level of each Customer the Bank shall on a regular basis:

a. Take appropriate measures to understand Customer's ownership and control structure, in particular with a view to gauging Beneficial Owner status (where applicable);
b. Obtain information about the purpose and intended nature of the business relationship;
c. Obtain information about the origin and destination of funds moved in connection with a business relationship or in the conduct of an occasional transaction, when justified by the Customer's risk profile or transaction characteristics;
d. Maintain ongoing monitoring of the business relationship to ensure that such transactions are consistent with the entity's knowledge of the Customer's activities and risk profile;
e. Maintain updated information obtained during the business relationship, which should be updated at least every five years in cases of lower risk, every three years in case of medium risk, every two years in cases of high risk and annually in cases of very high risk;
f. Whenever the risk analysis performed by the Bank to the business relationship or to the occasional transaction justifies that an aggravated level of knowledge of the Customer, their representative or beneficial owners is to be endorsed, the Bank asks for information or additional data which show adequate to the specifically found risk.

## Enhanced Due Diligence

An accountable institution must exercise ongoing due diligence in respect of all its business relationships which must, at a minimum, include:

- Maintaining adequate current and up-to-date information and records relating to the client and beneficial owner;
- Monitoring the transactions carried out by the client in order to ensure that such transactions are consistent with the accountable or reporting institution’s knowledge of the client, the client’s commercial or personal activities and risk profile; and
- Ensuring the obligations relating to high-risk clients and correspondent banking relationships are fulfilled.

An accountable institution must:

- Pay special attention to all complex, unusual large transactions and all unusual patterns of transactions which have no apparent economic or visible lawful purpose;

- Pay special attention to business relations and transactions with persons, including legal persons and trusts, from or in countries that do not or insufficiently apply the relevant international standards to combat money laundering and the financing of terrorism;
- Examine as far as possible the background and purpose of transactions and set forth in writing their findings;
- Keep the findings available for competent authorities and company auditors for at least seven years, or longer if specifically so requested by a competent authority before the expiration of the 7 years period;
- Conduct enhanced monitoring and due diligence when:
    i. any doubts arise about the veracity or adequacy of previously obtained customer identification data; or
    ii. there is a suspicion of money laundering or financing of terrorism; so as to prevent money laundering, financing of terrorism or the commission of any other offence.

An accountable institution which contravenes or fails to comply with this obligation commits an offence and is liable to a fine not exceeding N$100 million or to imprisonment for a period not exceeding 30 years, or to both such fine and such imprisonment.

## Beneficial Owner duties

Prior to the establishment of the business relationship or any occasional transaction (except in the cases listed above), the Bank assesses the status of the beneficial owner and collects at least the respective identifying data described above whenever:

a. The Customer, its beneficial owners, the business relationship or operation pose an increased risk of money laundering or terrorist financing;
b. The capacity of the beneficial owner(s) is (are) the person or natural persons who hold the top management of the Customer;
c. When acting as trustees or performing a similar function in explicit trusts or in unincorporated collective interests with similar structure or functions; or
d. This is determined by specific regulations or by the decision of the relevant sectoral authorities.

The Bank will also comply with the provisions of the preceding articles, whenever the Customer is a natural person who may not be acting on his own.

## Due identification duties in occasional transactions

Before undertaking an occasional transaction of more than N$99.999,99 the Bank must collect and record all information about the Customer and its Beneficial Owners (if applicable). All relevant identification data should always be verified through original supporting documents or certified copies of which the Bank must keep copies.
The Bank will verify the validity of the identification elements presented, regardless of whether they were already collected when a previous occasional transaction was undertaken.

Whenever the Bank proposes to conduct occasional transactions, in person or by means of distance communication, in national or foreign currency, of an amount equal to or greater than € 15,500, regardless of whether the transaction is undertaken in single or multiple transactions that appear to be related to each other or occasional transactions of any value for which they suspect a possible relationship to ML / TF, the Bank shall obtain at least the identification of the Customer and their respective representatives at the beginning and throughout the operation.

## Simplified identification and due diligence measures

The Bank may simplify the measures taken under the duty of identification and due diligence when it identifies a demonstrably reduced risk of money laundering and terrorist financing in business dealings, occasional transactions or the transactions they undertake.
The adoption of simplified due diligence measures is only permissible following a risk assessment by the Bank itself or by the regulator.
Simplified measures can never take place in any of the following situations:

a. When there is suspicion of money laundering or terrorist financing;
b. When enhanced identification or due diligence measures should be adopted;
c. Whenever determined by the Regulator.

## Enhanced identification and due diligence measures

The Bank shall reinforce the measures adopted under the duty of identification and due diligence when the Bank or any regulator identify an increased risk of money laundering or terrorist financing in business relations, occasional transactions or in operations undertaken.
Regarding the adoption of enhanced measures, the Bank shall define different degrees of risk which reflect the Bank's specific operative reality, contemplating at least the following aspects:

- Nature, dimension and complexity of the pursued activity;
- Respective Customers;
- Developed business areas, as well as regarding the products, services and available operations;
- Distribution channels of available products and services, as well as means of communication used to contact Customers;
- Countries or territories of origin of the Customers of the Bank, or in which they reside or, somehow, develop their activity at;
- Countries or territories where the Bank operates, directly or through third parties, belonging or not to the same group.

The revision of the high-risk degrees shall happen in a time interval which must not surpass the 12-month interval. However, this time interval might go up to the 24 month interval when the nature, dimension and complexity of the pursued activity justify it and the specific operative reality or the given area of business presents an inferior exposure to the ML/FT risk.

The Bank shall apply enhanced identification and due diligence measures when:

a. Occasional transactions or operations or otherwise related to natural and legal persons or similar persons located in high-risk third countries and offshore are carried out;
b. The establishment of the business relationship or the occasional transaction takes place without the Customer or his representative being physically present;
c. Customers, their representatives or Beneficial owners are Politically Exposed Persons;
d. The Bank identifies a situation of risk associated with a product, operation or distribution channel;
e. The Bank identifies jurisdictions associated with a higher risk of ML/FT linked to certain business relations or occasional transactions;
f. Cash deposits made by third parties in accounts held by Customers of the Bank.

Within the framework of enhanced identification and due diligence measures, especially regarding a politically exposed persons, the Bank shall:

a. Adopt appropriate procedures to determine whether the Customer may be considered a politically exposed person, and his or her actual residence, in the country or outside the national territory.
b. Adopt procedures for employees to obtain authorisation from the Compliance Department before establishing business relationships with such Customers;
c. Take necessary measures to determine the origin of the assets and funds involved in business relationships or occasional transactions;
d. Undertake continuous monitoring and enhanced due diligence in the business relationship with these entities under the analysis of the Head of Compliance or the MRLO.

Examples of reinforced measures include:

- Obtaining additional information about Customers, their representatives or Beneficial Owners, as well as about planned or performed operations;
- Assessment of their reputation;
- Information about their previously pursued activities;
- Assessment of close family members or strictly associated persons shall have a reference any Customer, representative or beneficial owner, even if the quality of PEP or of a person who pursues a public or political job has not been previously attributed;
- Additional steps to confirm the information obtained;
- Intervention from higher hierarchical levels within the Bank to authorise the establishment of business relationships and/or the execution of operations;
- The legitimacy of the funds involved in the business relationship or occasional transaction;
- The number, dimension or frequency of the transactions which the Bank estimates to happen throughout the business relationship;
- Intensifying the depth or frequency of business relationship monitoring procedures;
- The reduction of time intervals for updating information and other elements collected in performing identification and due diligence duties;
- Following up on the monitoring of the business relationship by the Regulatory Compliance Officer.
- The enforceability of the first payment referring to a given transaction by traceable means originating from a payment account, opened by the Customer with an entity which is not in a high-risk third country but has proved to apply identification and due diligence measures equivalent to those of the Bank;
- Assessment of the supporting documents of origin provided and the legitimacy of the Customers' assets, namely:
    - Income statements and, when applicable, wealth control;
    - Financial statement reports or accounts' legal certification;
    - Payroll statements;
    - Certificates extracted from public records;
    - Proving document of a succession acquisition;
    - Public information, including that from media outlets, as long as it is from an independent and credible source.
- When in higher-risk situations, the collecting of information regarding the connections established by the representative or the beneficial owner with other jurisdictions, as well as those established with associated persons, since might influence their operations. It can also be advantageous to collect information about the reason for establishing a business relationship or for conducting an occasional transaction outside their jurisdiction;
- Considering the adoption of the following enhanced measures in situations which require the presence of a higher risk associated with a product, operation of distribution channel:
    - Limitation of the number or amount of allowed operations;
    - Limitation of their usage to certain jurisdictions;

  - Limitation of their usage to certain types of Customers;
  - Limitation or restriction of cash deposits;
  - Demanding that cash deposits, account loadings, bank redemptions or reimbursements are performed via a trackable method, namely using the account opened at the Bank or at any other legally licensed entity which, even if not located in another high-risk country, implements similar measures to those established by the Act No. 13, 2012 and Act No. 3, 2007 and all adjacent regulations (e.g.: guidance; circulars; notices; directives; determinations and international regulations);
  - Parameterization of specific alerts in accordance with the product, service or operation's rated risk, by defining and implementing rules which allow the adjustment of the product, service or operation's risk when they are associated with high-risk Customers.
- Adoption of the following rules when the Bank identifies jurisdictions associated with a higher ML/FT risk regarding certain business relationships or occasional transactions:
  - Collect additional information about the given jurisdiction, namely about their legislative framework and the existence of supervision compatible with that established by the Act No. 13, 2012 and Act No. 3, 2007 and all adjacent regulations (e.g.: guidance; circulars; notices; directives; determinations and international regulations)Intensification of the depth of frequency of the monitoring procedures, taking specifically into consideration the origin and destination of the transactions.
- Considering the following factors in situations of high-risk correspondence relations:
  - Jurisdictions involved in the payment chain;
  - The complexity of the payment chain and the compensation systems used amongst entities which are authorized to provide financial services intervening in that payment chain;
  - The nature, dimension and number of intervening bodies in the payment chain, as well as jurisdictions where they operate;
  - Technology used for information transmission and the processing of operations in the payment chain;
  - Volume and amount of performed or to be performed transactions.

## Politically Exposed Persons

Under the Act and the Revised Guidance 01 of 2019 persons in this category carry an increased risk with regards to money laundering and terrorist financing, which justifies the implementation of special procedures for analysis and knowledge of the Customer – enhanced due diligence duty. This topic will be further developed in a separate section below.

## Risk countries

Some countries may qualify as "Risk Countries" due to political unrest, armed conflicts, high levels of organised crime, recognised involvement in the production or trafficking of drugs, etc. Maintaining business relationships with citizens of a Risk Country residing in that Country of Risk or who regularly engage in business with such countries may expose the Bank to greater risk.
The list of Risk Countries will be updated taking into account the reports of governmental or international organisations in this domain which divide risk countries into two groups: Very High-Risk

Countries and High-Risk Countries, and each time the Bank identifies jurisdictions associated with a higher ML/FT risk (Annex III).

### Professions/High-Risk Activity

This framework includes designated non-financial activities and professions, identified as higher risk and consequently subject to the duty of enhanced due diligence.
The Bank will not establish or maintain any relationship with Customers whose activities give rise to doubts regarding their legality.
The Bank will seek references from all new Customers. Referrals may come from a known Customer, a Bank employee, Bank shareholders, or companies within the same business group. Referred Customers do not exempt the Bank from performing the Customer's complete due diligence.

## 5. Politically Exposed Persons

The concept of Politically Exposed Persons (PEP), is described beneath, the concepts above will be interpreted by the Compliance Department under the laws in force in Namibia and international best practices and interpretations.

The Bank qualifies as PEP those entities present in accounts in which any of its interveners identified in the opening documents fall into this category or during the analysis of the account opening process the Compliance officer identifies the prospect as PEP.

The Head of Compliance or the MRLO after the analysis of the Compliance officer and the identification of the prospect as PEP or high-risk the process is verified by them for approval.

If in the course of its business relationship with the Bank, an account holder at any time falls into the category of PEP, the Compliance Department, upon becoming aware of this, and in the context of daily customer screening routines, shall immediately update the KYC referring to that particular Customer, and the Head of the Compliance Department or the MRLO must approve that classification later.

The relationships that the Bank establishes with PEP Customers must be reviewed biennially by the business area and submitted to the Compliance Department. In the case of policy framework, the Customer's position, or the nature of the actual relationship with the Customer changes considerably, the Bank must undertake a thorough and detailed review of the Customer’s records.

## 6. Document control and preservation

Business areas are responsible for obtaining all documentation required for account opening, including completed and signed forms. In cases where the account is subjected to the analysis of the Compliance Department, it is up to it to verify compliance with the requirements for opening an account and only in exceptional cases may it authorise the opening of an account in the process of which a document is missing, ensuring that the account is blocked until the situation is resolved. If the Compliance Department refuses account opening due to lack of requirements, it will always provide prompt reasons.
Records that relate to the establishment of a business relationship will be kept as long as the business relationship exists and for at least five years from the date on which the business relationship is terminated. Records that relate to single transactions will be kept for five years from

the date on which the transaction was concluded. Records that relate to copies of reports submitted to the FIC will be kept for a period of not less than five years from date of filing such report.

## 7. Operations analysis and control

Particular attention should be given to any transaction giving rise to suspicion of being related to money laundering or terrorist financing, regardless of its amount. For this purpose, the most common examples of suspicious laundering operations are listed in Annex I.
If the analysis concludes that there is reasonable evidence or certainty that the transaction is related to money laundering or terrorist financing practices, the transaction shall be immediately reported to the competent authorities.

### 7.1 Customer operations

The Bank conducts a periodical analysis of its Customers' transactions in each segment, using data extracted from the Bank's system, based on the Customers' risk level. The Bank will adopt measures that make it possible to determine the profile of each Customer in undertaking operations in order to identify deviant situations, to be analysed in more detail. Whenever necessary, the Compliance Department asks the business areas for additional information on each Customer's activity with the Bank.

The Compliance Department has in place transaction controls performed prior to its execution, as well as post-execution controls performed by the Compliance Department after the execution of the operation. Whenever the nature or volume of Customers' assets or liabilities operations do not correspond to their activity or operating history, the Compliance Department requests the business area to provide additional information regarding the origin and/or destination of the funds and their respective reasons.

Whenever the nature or volume of the transaction does not correspond to the Customer's activity and the above-mentioned source/destination information is not considered complete and clear by the business area, it should report the occurrence and report the Customer's operation to the Compliance Department.

The Bank will pay particular attention to situations in which funds are being credited to a single account, without cause for it, through cash deposits made by a large number of people.

In cases in which, during the exercise of its duty of examination, the Bank decides not to communicate the transaction to the competent authorities, it shall state in a document or register:

a. The grounds for the decision not to notify, including the reasons for the absence of any concrete factors of suspicion;
b. Reference to any informal contacts that may have been made during that examination with the Financial Intelligence Unit and with the judicial and police authorities, indicating the respective dates and means of communication used in those contacts.

The conclusions of the analysis, as described above, regarding the decision not to report a transaction should be kept for a minimum of 7 years and remain at the disposal of the auditors and supervisory and supervisory entities.

# 8. Target Financial Sanction

## 8.1. Asset Freeze

Under law no 97/2017 and Guidance note no 07 of 2023 among the applicable restrictive measures, the highlight given to the freezing of funds and economic resources.

Freezing of funds means preventing any move, transfer, alteration, use of, access to, or dealing with funds in any way that would result in any change in their amount, volume, location, ownership, possession, character, destination or any other change that would enable the funds to be used, including portfolio management.

Freezing of economic resources means preventing any move, transfer, sale or encumbrance of assets of every kind, whether tangible or intangible, movable or immovable, which are not funds but may be used to obtain funds, goods or services in any way, including, but not limited to, by selling, hiring or mortgaging them.
When an entity matches with one of the consolidated lists of persons, groups or entities subject to financial sanctions the Compliance Department blocks the account to prevent any movement and informs the authorities/regulators.

# 9. Communication suspicious operations

## Communication

Any transaction that may be suspected of being related to money laundering or terrorist financing, as well as any subsequent circumstances relating to such operations, should be immediately reported to the Compliance Department, which will act accordingly as regards compliance with the Duty to report to competent authorities.
The Bank shall also communicate to the Financial Intelligence Centre (FIC) on a systematic basis, any types of operations that are defined in the legislation in force.
The form, term, content and other terms of the systematic communications made by the Bank shall be in accordance with the applicable legislation.

## Communication procedure

A Bank employee who detects a suspected money laundering or terrorist financing operation shall immediately and concurrently report it to the head of their organisational unit and to the Compliance Department, that upon examination of the transaction, shall either notify or not inform the FIC. The communication procedure shall be done using the suspicious transaction reporting form.
The internal reporting procedure should be particularly rapid in ensuring compliance with legal rules requiring immediate reporting of the suspicious transaction to competent authorities.

## Content of communications

Reporting suspicious transactions should contain the following information:

a) Identification of the natural or legal persons participating in the suspicious transaction and the relationship between them;

b) A list of transactions and dates to which they relate, indicating their nature, currency in which they are carried out, amount, place or places of performance, purpose and payment or collection instruments used;
c) Invocation of evidence leading to suspicion indicating that the operation may be related to money laundering or terrorist financing.

## Informing the FIC

Whenever a suspicion about an operation is reported, the Compliance Department should give priority to reviewing it.
The Compliance Department will report any suspected money laundering or terrorist financing operations to the appropriate authorities.
Reports of suspicious transactions should be submitted via the FIC website.
Copies of all communications made under the reporting obligation shall be retained for a period of 7 years from the time such communication is made, as well as the respective supporting documents and a record of dates.

## Approval and Communication

This Policy is approved by the Board of Directors or the Executive Committee and enters into force on the next day after its approval.
This Policy will be made available to all employees through MetaCompliance.

## Revision

This Policy shall be reviewed annually or whenever deemed necessary by the Executive Committee or the Board of Directors in order to ensure compliance with the legal and regulatory rules to which the Bank is subject.
Changes to this Policy are subject to approval by the Board of Directors.

## ANNEX I

The supervisory authority issues guidelines containing examples of suspicious activities operations or other important scenarios.

It is a non-exhaustive list, and, on occasion, a single individual operation will not in itself be sufficient to arouse suspicion or to motivate internal investigations. However, any combination of the distinct casuistry of the operations presented may support the suspicion of illicit money laundering activities. The analysis should be made on a case-by-case basis, based on evidence of suspicion, in order to decide whether to inform the competent authorities, regardless of whether or not the transaction is included in this list.

## ANNEX II

## A non-exhaustive list of potentially higher risk factors and indicative types

### Customer Inherent Risk Factors:

- Business relationships that unfold in unusual circumstances;
- Customers resident or active in areas of higher geographical risk determined in accordance with paragraph 3 of this Annex;
- Legal persons, trusts or similar legal arrangements without a legal personality that are structures for holding personal assets

- Companies with nominee shareholders or those with their capital represented by bearer shares;
- Customers pursuing activities involving intensive cash transactions;
- Customer ownership or control structures that appear unusual or overly complex, given the nature of the Customer's activity.

Risk factors inherent in the product, service, operation or distribution channel:

- Private banking;
- Products or operations that may favour anonymity;
- Payments received from unknown third parties or associated with the Customer or the Customer's activity;
- New products and new business practices including new distribution mechanisms and payment methods, as well as the use of new technologies or developing technologies for both new and existing products.

Risk factors inherent in the geographical location:

- Countries identified by reputable sources, such as mutual assessment reports, detailed evaluation or follow-up reports, as having no effective systems for preventing and combatting money laundering and terrorist financing without prejudice to this law for high-risk third countries;
- Countries or jurisdictions identified by credible sources as having a significant level of corruption or other criminal activity;
- Countries or jurisdictions subject to additional sanctions, embargoes, other restrictive measures or countermeasures imposed by the United Nations and the European Union;
- Countries or jurisdictions that provide funding or support to terrorist activities or acts or in whose territory terrorist organisations operate.

## ANNEX III

## Low-risk jurisdictions or with regulations equivalent to the Portuguese Jurisdiction

- Member States of the European Union;
- Third countries with effective systems for preventing and combatting money laundering and terrorist financing;
- Countries or jurisdictions identified by credible sources as having a low level of corruption or other criminal activity;
- Third countries that are subject to anti-money laundering and counter-terrorism financing obligations based on credible sources, such as mutual assessment reports, detailed evaluation or follow-up reports, which are consistent with the revised recommendations from the FATF and effectively implement these obligations.

In the light of Community rules, the Member States of the European Union benefit from mutual recognition as regards their respective anti-money laundering and terrorist financing schemes.

## Countries/Jurisdictions at Risk for Money Laundering Prevention and Terrorist Financing

Very high risk and high-risk jurisdictions

High-risk jurisdictions are considered as jurisdictions referenced in the following indexes:

- Corruption Perceptions Index (latest version available);
- FATF / FATF - International Financial Action Task Force;
- AML Basel Index.

Offshore jurisdictions are also considered high risk jurisdictions in accordance with European regulation (namely EU Regulation 2016/1675 of 14 July 2016 from European Commission), as well as Notice no. 150/2004 of 13 February 2004 and Bank of Portugal's Notice no. 8/2016.

The list of jurisdictions and their associated risks can be found at the Banks internal portal, where it is regularly updated.