**AML/CTF Policy and Sanctions**

Policy on the Prevention of Money Laundering and Terrorist Financing (ML/TF), Proliferation of Weapons of Mass Destruction (PDAM) and Sanctions

| | |
|---|---|
| Date of Creation | 14 January 2025 |
| Date of Approval: | 28 January 2025 |
| Version: | 8 |
| Owner: | Compliance Department |
| Information Classification: | PUBLIC |
| Distribution List: | General Public |

## History of Changes

| Version | Date | Description of Changes | Department in Charge: | Reviewed by: | Approved by: |
|---|---|---|---|---|---|
| 1 | 17-08-2012 | - | CD | FGR | AE |
| 2 | 05-12-2014 | Addition of the following sections: 5. Customer Acceptance Policy and 6. Training Policy. Review of section 7. Responsibilities. | CD | FGR | AE |
| 3 | 20-03-2017 | Review of the following sections: 4. Policy on the prevention and detection of ML/TF, 5. Customer Acceptance Policy and 6. Training Policy. Section 8. Document retention was deleted, since it was included in section 4. | CD | FGR | AE |
| 4 | 08-02-2018 | Comprehensive review of the policy resulting from the implementation of the reinforcement of the internal control system to prevent money laundering and combat terrorist financing. | CD | FGR | CA |
| 5 | 28-11- 2019 | Review of section 2, iv, section 5 and Annex (Legal Framework) | CD | FGR | CA |
| 6 | 17-05-2022 | Review of the Purpose of the Policy regarding occasional transactions, the Customer Acceptance Policy and RCO as responsible for approving relationships with PEP's. | CD | FGR | CA |
| 7 | 15-12-2023 | Review of the legal and regulatory framework applicable to the Policy. Review of the Purpose of the Policy applicable to non-profit organisations and ARI, for the adoption of enhanced due diligence procedures. | CD | FGR | CA |
| 8 | 28-01-2025 | Full policy review: Addition of: key concepts; preventive duties, including a detailed description thereof; guidelines on management and monitoring of sanctions; clarification of simplified and enhanced due diligence measures; information about ML/TF risk management; and clarification of what is non-compliance with this Policy. | CD | SB | CA |

## Contents

***Copyright***

## 1 Introduction

BAI Europa, S.A. (hereinafter referred to as "BAIE" or "Bank"), in line with national and international standards and best practices applicable to its business sector, operates according to the highest standards of ethics and integrity, specially focused on preventing and combating money laundering and terrorist financing (ML/TF) and the Proliferation of Weapons of Mass Destruction (PWMD). In this regard, the adoption of preventive measures to combat ML/TF and PWMD is essential to the confidence of the financial system, and the Bank is strongly committed to developing skills and applying strict controls in this matter, requiring all employees to scrupulously comply with internally established procedures to prevent the use of the Bank's services for unlawful purposes.

The Bank is also committed to regularly monitoring national and international guidelines, standards and regulations regarding the fight against ML/TF and PWMD, in order to keep its internal standards and procedures permanently updated, in accordance with the best practices adopted in this matter.

## 2 Purpose of the Policy

This Policy defines the basic principles applicable to practices to combat ML/TF and PWMD, and therefore has the following objectives:

- Clarify the main relevant concepts and definitions adopted by the Bank, within the scope of the ML/TF Risk Management System (including the prevention and combat of the PWMD), which is integrated into the Bank's Risk Management System;
- Establish the guiding principles and rules to identify, assess, monitor, mitigate, control and report the ML/TF risk to which the Bank is, or may be, exposed, both internally and externally, in order to ensure that this risk remains at the previously defined level within the scope of the Bank's Risk Management;
- Identify the main duties and responsibilities of the various stakeholders in ML/TF Risk Management;
- Ensure, at all times, full compliance with the legislation, regulation, recommendations and guidelines issued by national, European and international entities applicable in terms of ML/TF risk management;
- Establish criteria for specific and regular training actions appropriate for Employees whose duties are relevant for the purposes of AML/CTF, so that they have adequate knowledge of the obligations arising from the existing regulatory framework, as well as the internal policies, procedures and controls defined by the Bank; and,
- Minimise the likelihood of situations of breach or non-compliance within the scope of AML/CTF and PWMD in relation to legislation, regulation, specific determinations, contracts, rules of conduct and relationship with Customers, established practices, ethical principles or other duties that may cause the Bank, or its Employees, to engage in illegal practices of an administrative, criminal and disciplinary nature, as well as in situation of potential reputational risk.

## 3 Glossary

For the purposes of this Policy, the following terms and expressions shall have the meanings set forth below:

**Law no. 83/2017, of 18 August** (hereinafter the Law): establishes measures to combat money laundering and terrorist financing.

**Money Laundering (ML):** any event designed to conceal the nature and origin of funds from illicit activities[1]. Money Laundering is considered to exist even when the activities that generate the assets occur in the territory of another State.

Money Laundering, as described above, is typically carried out through three (3) independent phases, namely:

i. Placement: the action of placing advantages obtained, directly or indirectly, through criminal activity into the financial system;
ii. Layering: action of converting the advantages obtained into another type of product, concealing the illegal origin through the creation of complex transaction structures and/or financial products;
iii. Integration: when the advantages obtained are introduced into the economy with a legitimate appearance.

**Terrorist Financing (TF):** collection of funds intended for terrorism, regardless of whether such funds originate from lawful activities. Terrorist Financing is considered to exist even when the provision or collection of funds or goods occurs in the territory of another State.

Contrary to the crime of Money Laundering, which aims to insert profits obtained from illicit activities into the legal economic-financial system, terrorist financing[2] has political, religious or ideological motivations, involving funds that are often much smaller and usually of lawful origin (e.g. donations or cash contributions to charities and non-profit organisations).

**Proliferation of Weapons of Mass Destruction (WMD):** refers to the development, production, acquisition, retention, transfer or use of nuclear, chemical and biological weapons, as well as their means of delivery, such as ballistic missiles, in order to increase the capacity for mass destruction, especially when in violation of international treaties or applicable regulations.

**Restrictive Measures (RM) or Sanctions:** set of measures adopted by the UNSC or the EU to freeze assets and economic resources related to terrorism, the proliferation of weapons of mass destruction and their financing, against a designated Person or Entity.

[1] This crime is provided for in Article 368-A of the Penal Code and is punishable by imprisonment of up to 12 years (in the case of an Obliged Entity, if the offence is committed in the exercise of its activity, imprisonment shall be up to 16 years).
In addition to the unlawful acts defined in Article 368-A of the Penal Code, the acts provided for in Article 2(1)(j) of the Law can also be included in the concept of money laundering.
[2] In the Portuguese legal system, the qualification of terrorist financing as an autonomous criminal offence is set out in paragraph 1 of Article 5-A of the Anti-Terrorism Law, and is punishable by imprisonment of 8 to 15 years.

**Beneficial Owner (BO):** the individual(s) who ultimately hold(s) ownership or control of the customer, and/or the individual(s) on whose behalf a transaction or activity is carried out, in accordance with the established criteria.

**Politically Exposed Persons** (**PEP**)[3]: individuals who perform, or have performed in the last 12 months, in any country or jurisdiction, prominent public function of a higher level, in accordance with the exhaustive list provided for in the Law. The enhanced identification and due diligence measures applied to entities that have this status must also apply/extend to:

- **Close Family Member of the PEP** (**CFM**): spouse or partner, parents and their spouse or partner (including stepmother and stepfather); children; siblings and their spouse or partner; grandparents and their spouse or partner; grandchildren and their spouse or partner; stepchildren and their spouse or partner; in-laws and their spouse or partner.
- **Relative Close Associate** (**RCA**)**:** any individual known as a co-owner with a politically exposed person, of a legal entity or a centre of collective interests without legal personality; or any individual who owns share capital or holds voting rights in a legal entity, or the assets of a centre of collective interests without legal personality, known as having a politically exposed person as its beneficial owner; or any individual known to have corporate, commercial or professional relationships with a politically exposed person.

**Holders of Other Political or Public Positions (HOPPP):** individuals who, not being qualified as Politically Exposed Persons, hold or have held, in the last 12 months and in national territory, the positions listed in Articles 2 and 3 of Law no. 52/2019, of 31 July, which approves the regime governing the exercise of duties by political officeholders and senior public officeholders.

**Residence Permit for Investment Activity (ARI),** also known as "Golden Visa": is an authorisation granted to a third-country national who requests residence or citizenship rights in Portugal in exchange for capital transfers, acquisition of assets or public debt securities or investment in corporate entities established in the national territory.

**Correspondent relationship**[4]: the provision of services by a bank, financial institution or other entity providing similar services (the correspondent), to: a bank, financial institution or other entity of an equivalent nature that is its client (the respondent), which includes the provision of a current account or other account that generates an obligation and related services, such as cash management, processing of money transfers and other payment services on behalf of the respondent, cheque clearing, payable-through accounts, exchange services and transactions with securities.

[3] The establishment or continuation of business relationships with PEP, CFM, RCA, HOPPP, ARI or clients whose beneficial owners fall into one of the aforementioned categories always depend on the prior authorisation of the Regulatory Compliance Officer or their substitute.
[4] The establishment of correspondent relationships is the subject of enhanced due diligence and, as such, requires a prior opinion by the DdC, among other obligations, before approval by the CA.

## 4 Stakeholders and Responsibilities

The Board of Directors (BoD) is responsible for setting internal policies and regulations regarding AML/CTF and PWMD, as well as defining, implementing and approving an organisational structure suitable for applying the procedures and controls in this regard.

Furthermore, the BoD is responsible for appointing the Regulatory Compliance Officer (RCO) who will monitor compliance with the legislation, regulation and the Bank's procedures in matters of AML/CTF and PWMD, taking into account skills, qualifications, academic background, training and professional experience.

The hiring of internal or external employees to perform duties that involve direct contact with customers, whether in person or remotely, as well as for the functional areas of control, compliance, AML/CTF and PWMD, risk management and internal audit, shall always be preceded by prior investigation into the history, curriculum and reputation of the candidates and approval by the Executive Committee (EC).

The process of permanent monitoring of the ML/TF risk management model shall be carried out within the scope of the Risk Management Monitoring Committee (CAGR).

The Compliance Department (CD) reports directly to the Director in charge of that matter (who, in turn, shares relevant/critical information with the BoD) and acts independently in fulfilling its responsibilities, namely in the implementation, monitoring and evaluation of internal procedures in matters of ML/TF and PWMD, as well as in centralising information and reporting suspicious transactions to the relevant authorities.

The Internal Audit Department (IAD) and External Audit perform, at least annually, control actions aimed at verifying compliance and effectiveness of the system established internally.

As part of its duties, the Supervisory Board (SB) is the body responsible for monitoring the conclusions of the aforementioned control assessment actions and the implementation of the identified recommendations for improvement, and, as a result of regulatory obligations, it must issue an annual opinion on the internal control system in matters of AML/CTF and PWMD.

The implementation of the recommendations identified following the assessment and control actions shall also be monitored by the BoD and the CAGR.

In short, the implementation of this Policy is the responsibility of the BoD, which delegates it to the CD.

## 5 Recipients

This Policy shall apply to all BAIE employees, in particular to all functional bodies responsible for the characterisation and supervision procedures related to AML/CTF and PWMD.

## 6 Guiding principles

a) The Bank implements an AML/CTF and PWMD prevention and detection programme that allows it to identify, monitor and prevent the practice of unlawful activities in the context of its operations;

b) The Bank identifies, assesses and mitigates the risks to which it is exposed, in accordance with the guidelines of the supervisory authorities, ensuring a proactive approach in managing the associated risks;

c) To ensure the effectiveness of the programme, the Bank carries out periodic reviews independently, assessing the enhanced or simplified due diligence measures adopted in relation to customers, ensuring that they are appropriate to mitigate the identified AML/CTF and PWMD risks;

d) Continuous monitoring of the quality, adequacy and effectiveness of the Bank's policies, procedures and controls regarding AML/CTF and PWMD is essential to ensure the robustness of the internal compliance system;

e) The programme is based on the identification and classification of risk sources, where potentially vulnerable areas are identified. The risk assessment is carried out annually on an individual basis, allowing adjustment of the controls established for each type of risk;

f) In combating ML/TF and PWMD, it is crucial to verify the information provided by customers or counterparties, as well as the autonomous collection of other information elements, according to the identified risks;

g) The Bank ensures that is employees have access to suitable, reliable and diversified sources of information, in accordance with the duties performed.

## 7 Preventive duties

The Bank, as an obliged entity, must comply with several preventive duties to prevent money laundering and terrorist financing and the proliferation of weapons of mass destruction, such as:

- Duty of Identification and Due Diligence;
- Duty of Refusal;
- Duty of Collaboration;
- Duty of Reporting;
- Duty of Abstention;
- Duty of Non-Disclosure;

- Duty of Examination;
- Duty of Control;
- Duty of Conservation; and,
- Duty of Training.

### 7.1 Duty of Identification and Due Diligence

The appropriate knowledge of its Customers by the Bank is an essential instrument to ensure the suitability of the products and services provided, but also to prevent the practice of ML/TF and PWMD crimes.

Consequently, the Bank, when establishing the business relationship and subsequently when updating information, or when carrying out occasional transactions, ensures scrupulous compliance with the legal and regulatory requirements in force at that time, which may ultimately lead to the exercise of the Duty of Refusal and/or the exercise of the Duties of Reporting or Abstention (described below).

With regard to the Duty of Identification and Due Diligence of Customers, Representatives and BO's, the Bank ensures it:

a) When establishing or maintaining a business relationship;
b) When carrying out occasional transactions;
c) Whenever there is a suspicion that the operations in question are related to the practice of ML/TF or PWMD crimes; or,
d) There are doubts about the veracity or adequacy of the customer identification data previously obtained.

The nature and scope of the procedures associated with the Duty of Identification and Due Diligence shall be adapted depending on the ML/TF risks specifically identified.

The identification and verification of the identity of (new or existing) Customers, their Representatives and BO's, regardless of the type of service provided, implies: (i) knowledge of a set of characteristics that include more than personal identification data, and, (ii) the collection of evidence, in compliance with legal and regulatory standards. Therefore, the identification, management and control of ML/TF follows a risk-based approach, and the Bank also adopts due diligence procedures in addition to the duty of identification, and their frequency is based on the level of risk of each customer.

The adoption of simplified or enhanced due diligence measures[5] is subject to the identification of criteria and signs of suspicion, in accordance with the illustrative list provided for in the Law and in the sectoral Regulation/guidelines.

[5] Examples of enhanced measures: transactions/operations with ARI's; PEPs, their family members and associates, as well as holders of other political or public positions; correspondent banking relationships; remote hiring; customers with a connection with a sanctioned/high-risk third country, Trade Finance operations, etc.

### 7.2 Duty of Refusal

The exercise of the Duty of Refusal applies when, in establishing and maintaining a business relationship, and in carrying out occasional transactions, it is not possible to obtain:

a) The identification elements and their means of proof provided for the identification and verification of the identity of the Customer, its Representative and the Beneficial Owner, including information for assessing the status of beneficial owner and the ownership and control structure of the Customer;
b) Information about the nature, subject matter and purpose of the business relationship;
c) Information that allows compliance with other identification and due diligence procedures.

The Bank terminates the business relationship, analyses the possible reasons for not obtaining the data, means of proof or information and, whenever the assumptions are met, assesses the need to report to the relevant authorities.

Whenever possible, the Bank must liaise with the relevant judicial and police authorities, consulting them in advance, when they have reasons to believe that the termination of the business relationship is likely to jeopardise the investigation.

### 7.3 Duty of Collaboration

The Bank, in exercising its Duty of Collaboration, provides prompt and full cooperation as requested by the Central Department of Investigation and Criminal Action (DCIAP) and the Financial Investigation Unit (UIF), as well as by the relevant judicial and police authorities, the sectoral authorities of the respective areas and also by the Tax and Customs Authority.

The exercise of this duty must be carried out in a timely manner, and may include fully and confidentially responding to requests for information, providing information, providing clarifications, providing documents, among others.

### 7.4 Duty of Reporting

Within the scope of the assessments carried out by the CD on entities and their ability to make transactions, whenever it considers that there is a suspicion of the practice of ML/TF and PWMD crimes, it must be immediately reported to the DCIAP and UIF, in accordance with the Law.

The reporting must cover all the activity considered suspicious, including transactions carried out, as well as those that have been suspended, blocked or refused by the Bank.

The Bank must ensure that the information and documentation relating to the reporting are archived, including the assessments and due diligence performed, and that they are made available to the sectoral authorities.

The decision to exercise the Duty of Reporting is the sole responsibility of the CD.

### 7.5 Duty of Abstention

The Bank must refrain from performing any transaction or set of transactions, present or future, that it knows or suspects may be associated with funds or other assets originating or related to the practice of criminal activities, terrorist financing or proliferation of weapons of mass destruction.

In the context of detecting a suspicious transaction or becoming aware of facts that indicate that a transaction may be related to the practice of a ML/TF and PWMD crime, this information must be submitted to the CD, which will follow the appropriate procedures.

### 7.6 Duty of Non-Disclosure

BAIE, including the members of its corporate bodies and its employees, regardless of their position and/or employment relationship, cannot disclose to the customer or to any third party: (i) any knowledge or suspicion that may lie with them, in terms of preventing ML/TF and PWMD; (ii) any information related to the duty of Reporting, including the content of such report; (iii) as well as any other information that may, directly or indirectly, impede the full exercise of the duties conferred on the obliged entities, or that jeopardise, in whole or in part, any investigations, enquiries, examinations, assessments or legal procedures and, in general, the prevention, investigation and detection of money laundering and terrorist financing and proliferation of weapons of mass destruction.

### 7.7 Duty of Examination

In the context of the assessment of transactions, there is a set of elements considered indicative of the practice of ML/TF and PWMD crimes, among others, which the Bank must take into consideration, namely:

a) The nature, purpose or atypicality of the transaction or activity;
b) Lack of an economic rationale;
c) The amounts operated in relation to the Customer's profile;
d) The jurisdictions involved;
e) The payment methods used; and,
f) The activity and profile of those involved in the transactions or activities.

Whenever, in the context of the assessment of transactions, it is found that a Customer's behaviour suggests engagement in activities or transactions that fall into the practice of ML/TF and PWMD crimes, or of another nature, measures are taken to intensify the level and nature of the monitoring carried out, in compliance with the Duty of Examination.

To support this examination/analysis, the Bank may request additional documentation to be provided, such as invoices, contracts, statements about the source of funds, among other documents. If, during the course of the investigations, the CD considers that the suspicion of the practice of ML/TF and PWMD crimes has been dispelled, it shall close the investigation, ensuring that the reasons for non-reporting, and the respective supporting documentation, are duly preserved. This decision must be subject to critical review by the BoD, after confirmation of non-reporting, and it may ultimately determine the reopening of the case.

### 7.8 Duty of Conservation

The Bank uses existing internal tools that allow the archiving of information and documentation, allowing the conservation of the assessments and due diligence carried out.

BAIE retains, for a period of seven (7) years, after the termination of the business relationship;

a) documentation and information obtained from the customer; and
b) other information obtained from public and reliable sources and/or other credible sources (public and reliable sources, e.g. adverse media, filtering systems, etc.)

This conservation must be permanently available to the relevant authorities, thus allowing the reconstruction of the transactions carried out and, consequently, the profile of transactions of the Customers.

### 7.9 Duty of Control

BAIE has implemented internal control policies and procedures, proportionate to its nature, dimension and complexity, and the business carried out by it, such as:

a) An effective risk management model, with practices appropriate to identify, assess and mitigate the risks of money laundering and terrorist financing and proliferation of weapons of mass destruction to which the obliged entity is or may be exposed;
b) Procedures and controls regarding customer acceptance;
c) Appropriate ongoing training programmes for the employees of the obliged entity, applicable from the moment they are hired, whatever the nature of their employment relationship;
d) Appointment of a Regulatory Compliance Officer (RCO);
e) Formal systems and processes for capturing, processing and archiving information;
f) Procedures for immediately monitoring designated individuals, groups or entities, ensuring compliance with restrictive measures adopted by the United Nations (UN), the Office of Foreign Assets Control (OFAC),

the European Union (EU) and other relevant entities. These measures include, among others, the freezing of funds, the prohibition of carrying out transactions and termination of business relationships with designated persons, groups or entities.

### 7.10 Duty of Training

BAIE adopts measures proportionate to the respective risks and the nature and dimension of its business so that its officers and other employees whose duties are relevant for the purposes of AML/CTF and PWMD are appropriately aware of the obligations arising from the Law and the regulations that implement it, including in terms of personal data protection.

To this end, BAIE ensures that specific training sessions are regularly offered to all employees, regardless of their role, professional category and/or employment relationship.

## 8 Due Diligence Measures

### 8.1 Simplified Due Diligence Measures

The Bank adopts, through its procedures, due diligence measures that allow it to complement the exercise of the Duty to Identify Customers, their Representatives or BO's, regularly and depending on the level of ML/TF risk attributed to it at a given time.

Therefore, before starting any business relationship or carrying out transactions, BAIE ensures compliance with due diligence measures that allow it to collect the necessary identification elements, in order to promote:

a) Confirmation and verification of the identity of the stakeholders, through the presentation of official and reliable documents;
b) The identification of the BOs if the business relationship or any proposed transaction;
c) The determination, in the case of a Legal Entity, of the ownership and/or control structure;
d) Information about the purpose or nature of the business relationship, ensuring its verification and continuous monitoring, in order to validate the context of the transactions carried out with the knowledge and experience it has of the Customer.

Examples of simplified measures adopted by the Bank:

- The identification, verification and proof of Customer's identity;
- Compliance with duties related to the identification of BOs, namely:
  - The assessment of their quality;
  - Obtaining information about their identity; and,

- The adoption of measures considered reasonable to verify their identity.
- Obtaining information about the purpose and nature of the business relationship;
- Continuous monitoring of the business relationship.

## 8.2 Enhanced Due Diligence Measures

The Bank ensures that the measures adopted are reinforced, in addition to the normal identification and due diligence procedures, under the Duty of Identification and Due Diligence, whenever an increased risk of ML/TF is identified in business relationships, in occasional transactions or in operations carried out.

The Bank applies enhanced due diligence measures, whenever the following situations occur:

a) Establishment of business relationships, performance of occasional transactions or performance of operations or relationships with Individuals or Legal Entities or Centres of collective interests without legal personality, established in third countries classified as high risk;
b) Establishment of business relationships or performance of occasional transactions with Customers, with their Representatives or BOs with PEP, CFM, RCA, HOPPP or ARI status;
c) Establishment of business relationships with Customers, with a high ML/TF risk score.

Additionally, when establishing a business relationship or performing an occasional transaction that takes place without the Customer or his/her/its Representative being physically present, BAIE may take additional due diligence measures to verify the relevant information and/or documents.

The Bank considers as examples of enhanced due diligence measures, without prejudice to others that may be more appropriate to the specific risks identified, the following measures:

a) Obtaining additional information from Customers, their Representatives or BOs;
b) Obtaining additional information about the transactions performed or to be performed;
c) Performance of additional due diligence to verify the information obtained;
d) Obtaining authorisation from higher hierarchical levels in establishing or maintaining business relationships with entities with PEP, CFM, RCA, HOPPP or ARI status;
e) The intensification of the depth or frequency of procedures for monitoring the business relationship or certain transactions, or set of transactions, with a view to detecting any indicators of suspicion of ML/TF and subsequent compliance with the duty of reporting, where applicable; and
f) Reducing the time intervals for updating information, depending on the Customer's risk.

## 9 Management and monitoring of Restrictive Measures/Sanctions

In order to pursue and comply with preventive duties, the Bank has implemented procedures and controls with a view to mitigating specific ML/TF risks, namely:

a) Filtering of entities subject to restrictive measures by the United Nations Security Council (UNSC), EU and OFAC;
b) Ensuring that all legal and regulatory requirements relating to financial sanctions are strictly and continuously complied with;
c) Ensuring that the automatic filtering systems used by the Bank comply with the objectives of identifying entities present in international lists, configuring correspondence percentages based on risk. It is also ensured that the filtering system is calibrated in accordance with the Bank's risk assessment;
d) Ensuring that the Bank's filtering systems take into account the latest lists of PEPs and sanctioned entities, namely listings from OFAC, UN, EU, among others, as well as lists provided by the regulator;
e) Ensuring that each and every employee of the Bank with responsibilities in updating exception lists and analysing system alert results, is aware and acts in accordance with the AML/CTF procedures established by the Bank.

Filtering shall be performed:

a) To all new customers and their relevant related parties;
b) When there are changes in the information of counterparties;
c) When the lists of Sanctions and PEPs are updated.

For the purposes of this Policy, it is established that, in addition to the possible self-declaration of a customer as a PEP or similar, the filtering system acts as a PEP identification control for subsequent classification with PEP status.

## 10 ML/TF Risk Management

In the context of the BCTF Global Risk Management Model, there are three (3) lines of defence:

**a) First line of defence**

The first line of defence is made up of the Commercial Area and the Operational Support Areas;

The Commercial Area is responsible for knowing and applying the obligations arising from this Policy, and must therefore:

i. Know the customer according to the acceptance criteria and continuous monitoring of the business relationship;
ii. Detect and report suspicious transactions in accordance with procedures for this purpose;

iii. Request exemption from the second line of defence, if it cannot meet the criteria of this Policy, as long as this does not violate the legal provisions in force;

iv. Collaborate with the second line of defence in implementing and improving due diligence control systems; and

v. Report possible risks and control deficiencies.

**b) Second line of defence**

The second line of defence is made up of the CD and the FGR, which are responsible for monitoring and carrying out a periodic assessment of the quality, adequacy and effectiveness of the policies, procedures and control systems implemented by the Bank, in terms of AML/CTF.

The CD, in fulfilling its responsibilities:

i. Reports its activity periodically to the Management Bodies and Regulatory Entities, namely to BdP;

ii. Systematically promotes advisory, review and control of the first line, with the purpose of ensuring that this Policy is correctly implemented;

iii. Develops and promotes the AML/CTF and PWMD culture and its integration into ML/TF risk management;

iv. In view of the risks previously identified by the first line of defence, the CD is responsible to take the necessary measures to mitigate them, confirming the existence of risks that may culminate in the exercise of the Duty of Abstention or Reporting.

**c) Third line of defence**

The third line of defence is made up of the DAI, which is responsible for monitoring the performance of the Bank's various functional areas, by periodically carrying out tests on the effectiveness of AML/CTF and PWMD Control Systems implemented by the Bank, as defined in the audit plan.

The DAI, within its scope of action, identifies shortcomings and opportunities for improvement, which are presented to the BoD and the SB, in order to keep the corporate bodies informed about these matters.

## 11 Customer Acceptance Policy

The Bank reserves the right not to accept customers (individuals or legal entities) or counterparties when they represent an unacceptable risk for the Bank, namely:

a) Shell banks or correspondent relationships with institutions that maintain relationships with entities that can be defined as such;
b) Entities with activities linked to the arms industry and diamond trade;
c) Currency exchange offices and entities that provide money transfer services;
d) Individuals or legal entities, including representatives and beneficial owners that have been subject to sanctions or restrictive measures imposed by the United Nations Security Council, the European Union or the OFAC;
e) Customers who refuse to provide/update identification elements, means of proof or other data requested by the Bank that aim to:
    (i) Identify the customer, legal representative, beneficial owner, management body;
    (ii) Understand the customer's ownership and control structure;
    (iii) Know the nature and purpose of the business relationship;
    (iv) Know the origin and destination of the funds;
    (v) Characterise the Customer's activity.
f) Customers who provide identification elements, means of proof or other information elements:
    (i) Not very credible as to their authenticity;
    (ii) Not very explicit as to their content;
    (iii) Difficult to confirm;
    (iv) With unusual characteristics.
g) Customers about whom the Bank has information disclosed by criminal or police investigation bodies, by the media, or by any other means, and which it finds to be related to criminal activities and suspicion of ML/TF;
h) Customers residing in countries subject to embargoes or other types of sanctions, and countries with strategic deficiencies in combating ML/TF.

The reasons for refusing to start or continue a business relationship are always analysed by the CD which, whenever necessary, will make the reports legally required for the situation in question.

## 12 Review, approval and dissemination

This Policy shall be reviewed annually or whenever the Bank's business circumstances, or when the legal or regulatory changes justify it.

The CD is responsible for updating this Policy, the Supervisory Board (SB) is responsible for reviewing it, by issuing a prior opinion, and the BoD is responsible for approving it.

Its internal dissemination to all Bank employees shall be carried out by the DEO-OEU (Department of Efficiency and Operations – Operational Efficiency Unit) and on the Bank's website by the MCU (Marketing and Communication Unit).

## 13 Non-compliance

Money Laundering, Terrorist Financing and Proliferation of Weapons of Mass Destruction are criminal offences foreseen and punishable in accordance with the Portuguese law, since any individual (including employees, corporate bodies or others) can be punished with effective imprisonment.

Administrative offence proceedings may also be initiated against the obliged entities (in this case, BAIE), which may result in large fines for failure to comply with laws and/or regulations, as well as other supplementary sanctions (e.g. from a warning to a ban on carrying out the business).

Without prejudice to the previous paragraphs, any breach of the rules established in this Policy may also result in the application of disciplinary sanctions, depending on the severity of the violation, the degree of guilt of the offender and the consequences of the act, which may range from a reprimand to dismissal with just cause.

## 14 General and regulatory framework

Laws, regulations, codes of conduct and other national and international best practices recognised in the areas of operation of the Bank were taken into account in the preparation of this Policy, such as:

- **Law no. 36/94**, of 29 September, establishing measures to combat corruption and economic and financial crime;
- **Law no. 5/2002,** of 11 January, establishing measures to combat organised and economic-financial crime, and makes the second amendment to Law no. 36/94, of 29 September, as amended by Law no. 90/99, of 10 July, and fourth amendment to Decree-Law no. 325/95, of 2 December, as amended by Law no. 65/98, of 2 September, Decree-Law no. 275-A/2000, of 9 November, and Law no. 104/2001, of 25 August;

- **Decree-Law no. 295/2003,** as amended by Decree-Law no. 61/2007, of 14 March, defining the concepts of resident and non-resident for the purposes carrying out foreign economic and financial transactions, as well as carrying out foreign exchange operations within the national territory;
- **Law no. 52/2003**, de 22 August (as amended by Law no. 25/2008, of 5 June, Law no. 17/2011, of 3 May and Law no. 60/2015, of 24 June), named Anti-Terrorism Act;
- **Law no. 83/2017**, of 18 August, establishing measures for combating money laundering and terrorist financing, partially transposing Directives 2015/849/EU, of the European Parliament and of the Council, of 20 May 2015, and 2016/2258/EU, of the Council, of 6 December 2016, amending the Penal Code and the Industrial Property Code, and repealing Law no. 25/2008, of 5 June, and Decree-Law no. 125/2008, of 21 July;
- **Law no. 89/2017,** of 21 August, approving the Legal Regime of the Central Register of Beneficial Owners, transposing Chapter III of Directive (EU) 2015/849, of the European Parliament and of the Council, of 20 May 2015, and amending Codes and other legal acts;
- **Law no. 97/2017,** of 23 August, governing the implementation and enforcement of restrictive measures approved by the United Nations or by the European Union, and establishing the penalty regime applicable to the breach of such measures. The most recent version is included in Law no. 58/2020, of 31 August;
- **Law no. 52/2019,** of 31 July, approving the regime for the exercise of duties by political officeholders and senior public officeholders;
- **Law no. 58/2020,** of 31 August, transposes Directive (EU) 2018/843 of the European Parliament and of the Council, of 30 May 2018, which amends Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of Money Laundering and Terrorist Financing;
- **Notice no. 7/2009**, of 1 September, prohibiting the granting of credit to entities based in offshore jurisdictions considered as non-cooperative or whose final beneficiary is unknown, defining offshore jurisdiction and non-cooperative offshore jurisdiction;
- **Notice no. 8/2016,** of 23 September, governing the obligations to register and report to Banco de Portugal the transactions corresponding to payment services whose beneficiary is a natural or legal person based in any offshore jurisdiction;
- **Notice no. 3/2020,** of 15 July, regulating governance and internal control systems, and defining the minimum standards on which the organisational culture of entities subject to the supervision of Banco de Portugal must be based;
- **Notice no. 1/2022**, of 5 May, repealing Banco de Portugal Notice no. 2/2018 and defining the conditions for the exercise, procedures, instruments, mechanisms, implementation formalities, obligations to provide information and other aspects necessary to ensure compliance with the duties to prevent money laundering and terrorist financing, within the scope of activity of the financial institutions subject to the supervision of Banco de Portugal;

- **Notice no. 1/2023**, of 24 January 2023, establishing the aspects necessary to ensure compliance with the duties to prevent money laundering and terrorist financing, within the scope of activity of entities that carry out activities with virtual assets. Amends Banco de Portugal Notice no. 1/2022, of 6 June.
- **Decree-Law no. 82/2024,** of 31 October, repealing Decree-Law no. 61/2007, of 14 March, which approves the legal regime applicable to the control of amounts of cash transported by individuals entering or exiting the EU through the national territory, as well as the control of cash transactions with other EU Member States, and makes the first amendment to Decree-Law no. 295/2003, of 21 November;
- **Ordinance no. 150/2004**, de 13 February, as amended by Ordinance no. 292/2011, of 8 November, and by Ordinance no. 345-A/2016, of 30 December, which published a list of countries, territories and regions with clearly more favourable tax regimes;
- **Ordinance no. 310/2018**, of 4 December, governing the provisions of Article 45 of Law no. 83/2017, of 18 August, defining the types of transactions to be reported by obliged entities to the Central Investigation and Criminal Action Department of the Attorney General's Office (DCIAP) and the Financial Information Unit of the Judicial Police (UIF), as well as the deadline, form and other terms of the reports;
- **Instruction no. 8/2024,** of 5 June, defining the required information to be reported annually to Banco de Portugal by financial institutions subject to its supervision with regard to the prevention of money laundering and terrorist financing, the respective model and other terms of submission;
- **Article 368-A of the Portuguese Penal Code,** as amended by Law no. 11/2004, defining that the crime of Money Laundering consists of the conversion, transfer, concealment or dissimulation of goods or products related to the trafficking of narcotics and psychotropic substances, pimping, sexual abuse of children or dependent minors, extortion, arms trafficking, trafficking of human organs or tissues, trafficking in protected species, tax fraud, influence peddling, corruption and other offences referred to in paragraph 1 of Article 1 of Law no. 36/94, of 29 September, and typical unlawful acts punishable by imprisonment of a minimum term exceeding 6 months or a maximum term exceeding 5 years;
- **Regulation (EC) no. 1889/2005** of the European Parliament and of the Council, of 26 October, on controls of cash entering or leaving the Community;
- **Regulation (EU) 2015/847** of the European Parliament and of the Council, of 20 May, on information accompanying transfers of funds, and repealing Regulation (EC) no. 1781/2006;
- **Commission Delegated Regulation** (EU) 2016/1675 of 14 July 2016, supplementing Directive (EU) 2015/849 of the European Parliament and of the Council, by identifying high-risk third countries with strategic deficiencies;
- **Circular Letter CEX/2022/1000041951**, of 6 May, establishing changes to the regime of the residence permit for investment (ARI) and implementation of enhanced due diligence measures;

- **EBA/GL/2023/03**, of 31 March, amending the EBA/2021/02 guidelines on customer due diligence and the factors that credit and financial institutions must take into account when assessing the risk of money laundering and terrorist financing associated with individual business relationships and occasional transactions.

In addition, the Bank's conduct also takes the form of a set of principles that are based on the best practices in the sector, namely with regard to the 40 FATF recommendations, the regulatory frameworks and best practices issued by the European Banking Authority (EBA), and also, where applicable, the Wolfsberg Questionnaire and the US Patriot Act.

## 15 Relationship with other documents

This Policy must be translated into procedures that contribute, as a whole, to strengthening the effectiveness of the Bank's AML/CTF system, so the information regarding AML/CTF is not limited to this document. Therefore, the Bank prepared a set of regulations that supplement the principles and objectives of this Policy into the Bank's operating reality.

- Risk Management Policy;
- Compliance Policy*;*
- Policy to Prevent and Combat Corruption;
- Policy on Reporting Irregularities;
- AMECB Standard and ML/TF Risk Prevention and Management Standard;
- Manual of Procedures – ML/TF Prevention.

**Approved by the Board of Directors on 28-01-2025**

| | | |
|---|---|---|
| Luís Lélis<br>Chair of the Board of Directors | Inokcelina de Carvalho<br>Non-Executive Director | César Gonçalves<br>Non-Executive Director - Independent |
| Omar Guerra<br>Chair of the Executive Committee | Nuno Leal<br>Executive Director | Henrique Gonçalves<br>Executive Director |