AML/CFT Policy and Sanctions

Policy on the Prevention of Money Laundering and Terrorist Financing (AML/CTF), Proliferation of Weapons of Mass Destruction (PWMD) and Sanctions

Date of Creation:	14 January 2025
Date of Approval:	16 March 2026
Version:	9
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 for the prevention of money laundering and countering terrorist financing.	CD	FGR	BoD
5	28-11- 2019	Review of section 2(iv), section 5 and Annex (Legal Framework).	CD	FGR	BoD
6	17-05-2022	Review of the purpose of the Policy regarding occasional transactions, the Customer Acceptance Policy and the RCO as the person responsible for approving relationships with PEPs.	CD	FGR	BoD
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	BoD
8	28-01-2025	Full review of the policy: Addition of: key concepts; preventive duties, including a detailed description thereof; guidelines on the management and monitoring of sanctions; clarification of simplified and enhanced due diligence measures; information on ML/TF risk management; and clarification of what constitutes non-compliance with this Policy.	CD	SB	BoD
9	11-03-2026	Full review of the policy, including: update of key concepts; clarification of the impact of the classification of customers as applicants for, or beneficiaries of, Residence Permits for Investment Activity within the scope of the management and monitoring of restrictive measures and sanctions; and review of the applicable legal and regulatory framework.	CD	SB	BoD

Contents

Copyright

1 Introduction

BAI Europa, S.A. (hereinafter referred to as "BAIE" or "Bank"), in line with the 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 maintaining confidence in 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 concerning the fight against ML/TF and PWMD, in order to keep its internal standards and procedures permanently up to date, 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 AML/CTF and PWMD, and therefore has the following purposes:

- 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 for identifying, assessing, monitoring, mitigating, controlling and reporting the ML/TF risk to which the Bank is, or may become, exposed, both internally and externally, in order to ensure that this risk remains at the level previously defined within the scope of the Bank's Risk Management;
- Identify the main duties and responsibilities of the various stakeholders involved 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 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 of 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 administrative, criminal and disciplinary offences, as well as in situations 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 intended to conceal the nature and origin of funds derived from unlawful activities[1]. Money Laundering shall be deemed to exist even where the activities that generated the assets occurred in the territory of another State.

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

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

Terrorist Financing (TF): the collection of funds intended for terrorism, regardless of whether such funds originate from lawful activities. Terrorist Financing shall be deemed to exist even where the provision or collection of funds or assets occurs in the territory of another State.

Unlike the crime of Money Laundering, which aims to introduce proceeds obtained from unlawful activities into the lawful economic and 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 (PWMD): refers to the development, production, acquisition, possession, transfer or use of nuclear, chemical and biological weapons, as well as their means of delivery, such as ballistic missiles, in order to increase mass destruction capacity, especially where in breach of

[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.

international treaties or applicable regulations.

Restrictive Measures (RM) or Sanctions: a set of measures of a political-diplomatic and non-punitive nature, adopted by the UNSC or the EU, against governments of third countries, non-State bodies, and natural and legal persons, with a view to maintaining or restoring international peace and security; protecting human rights; safeguarding democracy and the rule of law; preserving national sovereignty and independence and other fundamental interests of the State; and preventing and suppressing terrorism and the proliferation of weapons of mass destruction; for which purpose the freezing of assets and economic resources related to terrorism, the proliferation of weapons of mass destruction and their financing is imposed[3].

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

Politically Exposed Persons (**PEP**)[4]: individuals who hold, or have held in the last 12 months, in any country or jurisdiction, prominent public function of a senior level, in accordance with the exhaustive list provided for in the Law. The enhanced identification and due diligence measures applied to entities having this status must also be applied/extend to:

- **Close Family Members 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.

[3] Following the enactment of Law No. 70/2025, an amendment was made to Law No. 83/2017, notably the addition of the new Article 150-A on restrictive measures, which provides that the policies, procedures and internal controls created to ensure compliance with restrictive measures in the context of transfers of funds also extend to transfers of crypto-assets.

[4] 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.

Residence Permit for Investment Activity (*Autorização de Residência para Investimento*, ARI), also known as "Golden Visa": is an authorisation granted to a third-country national who applies for 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 national territory. Residence permits for entrepreneurial immigrants (D2 visa) shall be treated as equivalent thereto, and classification as an ARI beneficiary shall extend to family members who, by means of family reunification, are also deemed to benefit from that status.

Correspondent relationship[5]: 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, foreign exchange services and securities transactions, transfers of crypto-assets or other transactions involving crypto-assets.

Crypto-asset: a digital representation of a value or of a right that can be transferred and stored electronically, using distributed ledger technology or similar technology, within the meaning of point 5 of Article 3(1) of Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May on markets in crypto-assets.

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 Bank's legislation, regulations and procedures on 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).

[5] The establishment of correspondent relationships is the subject of enhanced due diligence and, as such, requires a prior opinion by the CD, among other obligations, before approval by the BoD.

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 (RMMC).

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 RMMC.

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 of 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 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 issued by 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 independent reviews, assessing the enhanced or simplified due diligence measures adopted in relation to customers and ensuring that they are suitable for mitigating the AML/CFT and PWMD risks identified;

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

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

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

g) The Bank ensures that its 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 relating to the prevention of 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 Retention; and
- Duty of Training.

7.1 Duty of Identification and Due Diligence

The Bank's appropriate knowledge of its customers is an essential instrument for ensuring the suitability of the products and services provided, but also for preventing the commission of ML/TF and PWMD offences.

Accordingly, when establishing a business relationship and subsequently when updating information, or when carrying out occasional transactions, the Bank ensures scrupulous compliance with the legal and regulatory

requirements in force at the 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 de of Customers, Representatives and BOs, the Bank ensures compliance therewith:

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 commission of ML/TF or PWMD offences; or
d) Where 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 according to the ML/TF risks specifically identified.

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

The adoption of simplified or enhanced due diligence measures[6] is subject to the identification of criteria and signs of suspicion, in accordance with the illustrative list provided for in the Law and in sectoral regulations/guidelines.

7.2 Duty of Refusal

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

a) The identification data and respective supporting evidence required 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 Customer's ownership and control structure;
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.

[6] Examples of enhanced measures include transactions/operations involving ARIs; PEPs, their family members and associates, as well as holders of other political or public positions; correspondent banking relationships; remote onboarding; customers with a connection to a sanctioned country/high-risk third country; Trade Finance operations, etc.

The Bank terminates the business relationship, analyses the possible reasons for failure to obtain the data, evidence or information and, whenever the relevant conditions are met, assesses the need to report to the respective authorities.

Whenever possible, the Bank must liaise with the relevant judicial or police authorities, consulting them in advance whenever it has reasons to believe that termination of the business relationship may jeopardise an investigation.

7.3 Duty of Collaboration

In exercising the Duty of Collaboration, the Bank provides prompt and full cooperation as requested by the Central Department of Investigation and Criminal Prosecution (*Departamento Central de Investigação e Ação Criminal*, DCIAP) and the Financial Intelligence Unit (*Unidade de Investigação Financeira*, UIF), as well as by the relevant judicial and police authorities, the sectoral authorities for the respective areas and also by the Tax and Customs Authority.

This duty must be performed 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 commission of ML/TF and PWMD offences, 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 filed, 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, which it knows or suspects may be associated with funds or other assets derived from or related to criminal activities, terrorist financing or the proliferation of weapons of mass destruction.

In the context of detecting a suspicious transaction or becoming aware of facts indicating that a transaction may be related to the commission of a ML/TF and PWMD offence, 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 relation to the prevention of 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, hinder the full performance of the duties conferred on the obliged entities, or that may jeopardise, in whole or in part, any investigations, inquiries, 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 commission of ML/TF and PWMD offences, among others, which the Bank must take into consideration, namely:

a) The nature, purpose or atypical nature of the transaction or activity;
b) The absence 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 involvement in activities or transactions that fall into the commission of ML/TF and PWMD offences, 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 retained. 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 Retention

The Bank uses the existing internal tools that allow information and documentation to be filed, enabling the retention of the assessments and due diligence performed.

BAIE retains, for a period of seven (7) years after 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 retained information must be permanently available to the relevant authorities, thus allowing the reconstruction of the transactions carried out and, consequently, the Customer's transactional profile.

7.9 Duty of Control

BAIE has implemented internal control policies and procedures, proportionate to its nature, size and complexity and to the activity it carries out, such as:

a) An effective risk management model, with practices suitable for identifying, assessing and mitigating the risks of money laundering and terrorist financing and the proliferation of weapons of mass destruction to which the obliged entity is or may become exposed;
b) Procedures and controls regarding customer acceptance;
c) Appropriate ongoing training programmes for the obliged entity's employees, applicable from the time such employees are admitted, regardless of the nature of their employment relationship;
d) Appointment of a Regulatory Compliance Officer (RCO);
e) Formal systems and processes for collecting, processing and filing information;
f) Procedures for immediately monitoring and identifying designated individuals, groups or entities, ensuring compliance with the restrictive measures adopted by the United Nations (UN), the Office of Foreign Assets Control (OFAC), the European Union (UE) and other relevant entities. These measures include, among others, the freezing of funds, the prohibition on carrying out transactions and the termination of business relationships with designated individuals, groups or entities.

7.10 Duty of Training

BAIE adopts measures proportionate to the relevant risks and to the nature and size of its business so that its officers and other employees whose duties are relevant for AML/CTF and PWMD are appropriately aware of the obligations arising from the Law and the regulations implementing 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 supplement the exercise of the Duty of Identification of Customers, their Representatives or BOs, regularly and according to the level of ML/TF risk assigned to them at any given time.

Therefore, before establishing any business relationship or carrying out transactions, BAIE ensures compliance with due diligence measures enabling it to collect the necessary identification data, in order to promote:

a) Confirmation and verification of the identity of the stakeholders, through the presentation of official and reliable documents;

b) Identification of the BOs of the business relationship or of any proposed transaction;

c) Determination, in the case of a Legal Entity, of the ownership and/or control structure;

d) Information on 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 against the knowledge and experience it has of the Customer.

Examples of simplified measures adopted by the Bank:

a) Identification, verification and proof of the Customer's identity;

b) Compliance with the duties related to the identification of BOs, namely:

   i. The assessment of their quality;

   ii. Obtaining information about their identity; and

   iii. Adoption of measures considered reasonable to verify their identity.

c) Obtaining information about the purpose and nature of the business relationships;

d) Ongoing monitoring of the business relationships.

8.2 Enhanced Due Diligence Measures

The Bank ensures that the measures adopted are enhanced, in addition to the normal identification and due diligence procedures, under the Duty of Identification and Due Diligence, whenever an increased ML/TF risk is identified in business relationships, occasional transactions or operations it carries 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 transactions 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, their Representatives or BOs who have 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 their Representative being physically present, BAIE may take additional due diligence measures to verify the relevant information and/or documents.

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

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 for the establishment or maintenance of business relationships with entities that have PEP, CFM, RCA, HOPPP or ARI status;
e) Intensifying the depth or frequency of the 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 subsequently complying with the duty of reporting, where applicable; and
f) Reducing the time intervals for updating information, according to the Customers' 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 aimed at mitigating specific ML/TF risks, namely:

a) Screening of entities subject to restrictive measures imposed by the United Nations Security Council (UNSC), the EU and OFAC;
b) Ensuring that all legal and regulatory requirements relating to financial sanctions are complied with strictly and continuously;
c) Ensuring that the automatic screening systems used by the Bank meet the objectives of identifying entities included in international lists, by setting matching percentages according to risk. It is also ensured that the screening system is calibrated in accordance with the Bank's risk assessment;
d) Ensuring that the Bank's screening systems take into account the most up-to-date lists relating to PEPs and sanctioned entities, namely the OFAC, UN and EU lists, among others, as well as lists provided by the regulator;
e) Ensuring that each and every Bank employee with responsibilities within the scope of updating exception lists and analysing system alert results is aware of, and acts in accordance with, the AML/CFT procedures established by the Bank.

Screening shall be carried out on:

a) All new customers and their relevant related parties;
b) Whenever there are changes to counterparty information;
c) Whenever the Sanctions and PEP lists are updated.

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

It should also be highlighted, in this context, that information relating to customers who are beneficiaries of (or applicants for) a Residence Permit for Investment Activity (ARI) must be checked against restrictive measures, in order to identify or properly assess situations in which ARI customers or other parties use passports of alternative nationalities, legal structures or highly complex transactions – characterised, namely, by the use of multiple financial institutions, accounts, intermediaries, financial operations or jurisdictions – with the potential to conceal links to individuals or entities subject to restrictive measures. It is reiterated that applying for or holding an ARI does not constitute an exception to compliance with restrictive measures, which must be observed regardless of the customer's immigration status.

10 ML/TF Risk Management

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

a) First line of defence

The first line of defence consists 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 in accordance with the acceptance criteria and ongoing monitoring of the business relationship;

ii. Detect and report suspicious transactions in accordance with the procedures established for this purpose;

iii. Request a waiver from the second line of defence if it is unable to comply with the criteria of this Policy, provided that this does not breach the legal provisions in force;

iv. Cooperate 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 consists 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 relation to AML/CTF. In performing its responsibilities, the CD:

i. Periodically reports its activity to the Management Bodies and Regulatory Entities, namely to BdP;

ii. Systematically provides advisory, review and control support to the first line, with the aim of ensuring that this Policy is correctly implemented;

iii. Develops and promotes an AML/CFT 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 for taking the necessary due diligence 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 consists 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.

Within the scope of its activity, the DAI identifies shortcomings and opportunities for improvement, which are submitted to the BoD and the SB, in order to keep the corporate bodies informed on these matters.

11 Customer Acceptance Policy

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

a) Shell banks or correspondent relationships with institutions that maintain relationships with entities that may be defined as such;
b) Entities with activities linked to the arms business and diamond trade;
c) Currency exchange offices and entities providing money remittance services;
d) Individuals or legal entities, including representatives and beneficial owners, who 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 data, supporting evidence or other data requested by the Bank that aim to:
    i. Identify the customer, legal representative, 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 data, supporting evidence or other information:
    i. Not very credible as to their authenticity;
    ii. Not very clear as to their content;
    iii. Difficult to confirm;
    iv. With unusual characteristics.

g) Customers in relation to whom the Bank has information disclosed by criminal or police investigation bodies, by the media, or by any other means, and which the Bank considers to be related to criminal activities and suspicions 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 commence or continue a business relationship are always analysed by the CD, which, whenever necessary, shall make the legally required reports for the situation in question.

12 Review, Approval and Dissemination

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

Accordingly, 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.

It shall be disseminated by the DEO-UEO (Department of Efficiency and Operations – Operational Efficiency Unit) to all Bank employees and shall be available for consultation on the QPR Portal and on the Bank's website if the document classification is "Public".

13 Non-Compliance

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

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

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

14 General Legal and Regulatory Framework

Laws, regulations, codes of conduct and other recognised national and international best practices in the sectors in which the Bank operates 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 making the second amendment to Law No. 36/94, of 29 September, as amended by Law No. 90/99, of 10 July, and the fourth amendment to Decree-Law No. 325/95, of 2 December, as amended by Law No. 65/98, of 2 September, by Decree-Law No. 275-A/2000, of 9 November, and by 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 of carrying out foreign economic and financial transactions, as well as foreign exchange transactions in national territory;
- **Law No. 52/2003**, of 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), known as the Anti-Terrorism Law;
- **Law No. 23/2007**, of 4 July (19th version, resulting from the amendment introduced by Law No. 61/2025, of 22 October), approving the legal regime governing the entry, stay, exit and removal of foreigners from national territory;
- **Law No. 83/2017**, of 18 August, establishing measures to combat 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 the European Union and establishing the sanctions regime applicable to breaches of such measures. The most recent version is set out in Law No. 72/2025, of 23 December;
- **Law No. 52/2019**, of 31 July, approving the regime governing the exercise of duties by political officeholders and senior public officeholders;
- **Law No. 58/2020**, of 31 August, transposing 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;

- **Law No. 70/2025**, of 22 December, implementing in the domestic legal system Article 38 of Regulation (EU) 2023/1113 on information accompanying transfers of funds and certain crypto-assets, and amending Law No. 83/2017, of 18 August;
- **Notice No. 7/2009**, of 1 September, prohibiting the granting of credit to entities based in offshore jurisdictions considered non-cooperative or whose ultimate beneficiary is unknown, defining offshore jurisdiction and non-cooperative offshore jurisdiction;
- **Notice No. 8/2016**, of 23 September, governing the duties to register and report to Banco de Portugal transactions corresponding to payment services whose beneficiary is an individual or legal entity 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, information reporting obligations and other aspects necessary to ensure compliance with the preventive duties relating to money laundering and terrorist financing within the scope of activity of financial entities 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 preventive duties relating to money laundering and terrorist financing within the scope of the activity of entities providing crypto-asset services (terminology amended by Law No. 70/2025). It 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 leaving the European Community through national territory, as well as to 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**, of 13 February, as amended by Ordinance No. 292/2011, of 8 November, and by Ordinance No. 345-A/2016, of 30 December, which published the 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 Intelligence Unit of the Judicial Police (UIF), as well as the deadline, form and other terms of such reports;
- **Instruction No. 8/2024**, of 5 June, defining the required information to be reported annually to Banco de Portugal by financial entities subject to its supervision in relation 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, which provides that the crime of Money Laundering consists of the conversion, transfer, concealment or disguise of assets or products related to trafficking in narcotic drugs and psychotropic substances, pimping, sexual abuse of children or dependent minors, extortion, arms trafficking, trafficking in human organs or tissues, trafficking in protected species, tax fraud, influence peddling, corruption and other offences referred to in Article 1(1) of Law No. 36/94 of 29 September, and typical unlawful acts punishable by imprisonment for a minimum term exceeding 6 months or a maximum term exceeding 5 years, including, as a result of the addition introduced by Law No. 72/2025, breach of restrictive measures;
- **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;
- **Regulation (EU) 2023/1113** of the European Parliament and of the Council of 31 May on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849;
- **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 CC/2026/00000005** of 30 January, establishing guidelines on the measures and procedures to be adopted in relation to the risks associated with business relationships and occasional transactions whose customers or associated persons are applicants for or beneficiaries of residence permits for investment activity (ARI);
- **Circular Letter CC/2020/00000063** of 27 November, concerning the application of enhanced measures in the context of the use of companies incorporated using expedited means for the creation of companies for money laundering practices;
- **EBA/GL/2023/03** of 31 March, amending Guidelines EBA/2021/02 on customer due diligence and the factors which credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions.

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

15 Relationship with other documents

This Policy shall be translated into procedures which, as a whole, contribute to strengthening the effectiveness of the Bank's AML/CTF system; accordingly, the information relating to AML/CTF is not limited to this document. The

Bank has therefore prepared a set of regulations that supplement the principles and objectives of this Policy in the Bank's operational reality.

- Risk Management Policy;
- Compliance Policy;
- Policy on Preventing and Combating Corruption;
- Policy on Reporting Irregularities;
- AMMECB and ML/TF Risk Prevention Standard;
- Manual of Procedures – ML/TF Prevention.

Approved by the Board of Directors on 16-03-2026

Luís Lélis Chair of the Board of Directors	Inokcelina de Carvalho Non-Executive Director	Irisolange Verdades Non-Executive Director
César Gonçalves Non-Executive Director - Independent	Omar Guerra Chair of the Executive Committee	Miguel Costa Santos Executive Director
Henrique Gonçalves Executive Director		