Group Policy
Relating to the Prevention of Money Laundering and Terrorism Financing

1. PURPOSE AND SCOPE OF POLICY

The Bank of Cyprus Public Company Ltd (BoC) is committed to the highest standards in the fight against money laundering and terrorism financing and institutes appropriate procedures to comply fully with relevant legislation, regulations, guidelines and best practices, and exercises due diligence to deter the use of its services and products by money launderers and those involved in illegal activities including the financing of terrorism.

All members of the staff across BoC have an individual and personal responsibility to comply with Anti Money Laundering and Combating Terrorism Financing legislation and regulations. Failure to comply may lead to disciplinary action against a member of staff in fault.

BoC examines its AML/CTF strategies, policies, procedures, and programs on an ongoing basis and retains an effective AML program for BoC's business ensuring compliance with all applicable legal and regulatory requirements. Furthermore, additional regulations on specific issues may be set by BoC, from time to time, to streamline policy implementation and avoid possible conflicts between country regulations.

The purpose of this policy is to set the minimum standards and provide general guidance and clarity on BoC's effort to prevent and suppress money laundering, terrorist financing and other illegal activities and to ensure compliance with all applicable legal and regulatory requirements.

The main objectives of the principles incorporated in this Policy are:

1. Take all reasonable steps and exercise Due Diligence to deter the use of BoC's systems and processes by money launderers and those involved in criminal and illegal activities including the Financing of Terrorism.
2. Avoid violations, since they may result in criminal, civil and regulatory sanctions and/or penalties/fines imposed.
3. Protect BoC's reputation by protecting BoC and its employees from unfounded allegations of facilitating Money Laundering and Terrorist Financing.
4. Create a high standard of compliance culture among all the staff across BoC.

BoC ensures that the legal and regulatory requirements stemming from the provisions set out in the Law 188(I) 2007, the 6th edition of the Central Bank of Cyprus Directive for the prevention of Money Laundering and Terrorist financing and the 1st edition of the Central Bank of Cyprus Directive for Compliance with the Provisions of UN Security Council of the European Union, are addressed by BoC.

All BoC Group entities are expected to enact in their own internal systems equivalent procedures. Corresponding Bank functions have the responsibility for coordinating the application of the framework across BoC, in accordance with established reporting lines.

2. ABBREVIATIONS

Within this document, the following abbreviations are used:

Abbreviation	Definition
AML	Anti-money Laundering
AMLCO	Anti-Money Laundering Compliance Officer
BoC	Bank of Cyprus Public Company Ltd
BoC Group	Bank of Cyprus Public Company Ltd and its subsidiaries
BoC Group Entities	Bank of Cyprus Public Company Ltd subsidiary
CBC	Central Bank of Cyprus
CTF	Combating Terrorism Financing
DPO	Data Protection Officer
EBA	European Banking Authority
FC&SCD	Financial Crime & Sanctions Compliance Department
FIU	Financial Intelligence Unit
ICAAP	Internal Capital Adequacy Assessment Process
KYC	Know Your Customer
KYCB	Know Your Customer's Business
Law	The Prevention and Suppression of Money Laundering and Terrorist Financing Activities Law of 2007 (Law 188(I)/2007)
ML / TF	Money Laundering / Terrorism Financing
RCSA	Risk and Control Self-Assessment

3. DEFINITION OF TERMS

1. **Know Your Customer (KYC)**

   It is the Due Diligence process that BoC performs to identify its clients and ascertain relevant information pertinent to doing financial business with them. The main components are the following:

   a. **Customer Acceptance Policy** - As per BoC's Customer Acceptance Policy, BoC recognizes that the evaluation of a customer's risk is fundamental in its effort to prevent and suppress money laundering, terrorist financing and other illegal activities. Hence, BoC defines:

      i. a list of persons (physical and/or legal), accounts or transactions that are not accepted,

      ii. a list of parameters/criteria which are considered by the automated AML scorecard to determine the risk level of prospect and current customers,

      iii. a list of persons classified as High-Risk Customers (physical and/or legal) in accordance with the requirements of the Central Bank AML Directive. For those persons and for persons classified by the AML scorecard as high risk, special authorization from Senior Management is required prior to the establishment of any business relationship.

      iv. a list of conditions under which a business relationship with an existing client is terminated.

   BoC develops policies and procedures that provide for enhanced due diligence for high and significant risk customers, in accordance with the provisions of the Law 188(I) 2007 and all amendments that

followed and the 6th edition of the Central Bank of Cyprus Directive for the prevention of Money Laundering and Terrorist financing.

b. **Customer Identification** - The identification of the customer includes the collection of all relevant documents and information that result not only in the identity of the customer, and subsequently the ultimate beneficial owner, but additionally in the creation of the economic profile of the customer including the nature of its business activities (KYCB). During customer identification, the customer is filtered against known lists to establish whether this customer is under any sanctions or has any negative press information or is a Politically Exposed Person.

c. **Continuous/On-going Monitoring** - The customers and their accounts are continuously monitored using BoC's AML systems, as well as through the adherence to relevant procedures to identify unusual or suspicious transactions and where necessary report these to the authorities.

d. **AML Risk Management** - KYC and KYCB procedures include measures such as, adequate monitoring systems and controls, close monitoring, regular review process, segregation of duties, staff training and specialized AML systems.

2. Money Laundering

It refers to the participation in any transaction that seeks to conceal or disguise the nature or origin of funds derived from illegal activities. It is the process by which criminals attempt to conceal the true origin and ownership of the proceeds of criminal activities. If successful, the money can lose its criminal identity and appear legitimate. The definitions covers the cases where the acts which generated the relevant assets were perpetrated in another jurisdiction, if such acts would constitute an offence had they been perpetrated in the jurisdiction of the local Bank Entity and are considered punishable under the laws of the said jurisdiction. BoC can be severely exposed by failing to successfully implement its AML/CTF program. Apart from the reputational risk, the Regulator may impose fines, sanctions and even proceed with the suspension or cancellation of banking licenses. It is noted that the Cyprus AML Law defines and criminalizes money laundering deriving from all serious criminal offences, which constitute offences punishable with imprisonment exceeding one year, including tax offenses relating to direct or indirect taxes.

3. Regulated Subsidiary

A subsidiary of BoC which falls under the definition of an "obliged entity" under the Cyprus AML Law, namely CISCO , Eurolife and JCC.

4. Terrorist finance

It is defined as the act of providing any material or facilities or the collection, financing or managing of funds aiming to perform, facilitate or assist the commission of a terrorist act by a criminal organization or individual terrorist.

4. GENERAL PRINCIPLES

4.1 General Principles

Each BoC Group entity complies with the following Bank's general AML/CTF policies, principles and practices:

1. Apply the principle of proportionality in conducting its operations. In this respect, the Bank tailors its AML/CTF controls to the nature, scale, and risk level of its activities and customers. The factors that are considered include the Bank's legal form, group structure, business model, organizational and ownership structure, size (assets, turnover, employees), and geographical presence. By assessing these, BoC ensures AML/CTF measures are effective, targeted, and compliant.

2. Maintain appropriate comprehensive procedures on AML/CTF, including detailed circulars and controls for the effective implementation of its AML/CTF policy. The following elements are clearly documented within the procedure circulars and manuals and within the risk management framework of the Bank:

    - Formal risk assessment frameworks, defining risk appetite and conducting both business-wide and customer-specific assessments.
    - Customer Acceptance Policy related procedures.

      Procedures ensuring thorough identification and verification of all customers and beneficial owners and establishment of the nature and intended purpose of the business relationship
    - Ongoing monitoring and updating the customer profile, which should be risk-based, depending on the circumstances.
    - In cases where simplified due diligence is applied for the certification and verification of a customer's identity, how, and in which situations, these are compensated through enhanced monitoring.
    - The detection and reporting of unusual and/or suspicious transactions to the AMLCO and the FIU.
    - Record-keeping procedures.
    - The procedures complying with the Regulation (EU) 2023/1113,
    - Protection of personal data.

The DPO is involved in all processes relating to the processing and protection of personal data.

3. Adopt and apply a risk-based approach towards ML/TF risks. This approach enables BoC to identify, assess, and mitigate money laundering and terrorist financing risks proportionately and effectively. Risk assessments are conducted at both the individual and business-wide levels, considering key risk factors and assessment on the following:

    a. country risk, based on jurisdictional exposure and geopolitical concerns
    b. product risk, reflecting the inherent vulnerabilities of financial products and services
    c. customer risk, legal form and structure
    d. industry risk, based on sector-specific exposure to illicit finance
    e. transaction risk, considering the nature, volume, and complexity of financial activity
    f. distribution channel risk, assessing the method of service delivery and its susceptibility to misuse

These factors guide the application of customer due diligence (CDD), enhanced due diligence (EDD), and ongoing monitoring measures, ensuring compliance is both targeted and proportionate. Regular risk assessments guide the implementation of appropriate controls and mitigation measures.

4. Conduct regular assessments of the effectiveness of its AML/CFT framework, including the risk management assessment processes, customer due diligence procedures, transaction monitoring systems, and internal controls.

5. The main categories which BoC classifies the customers in terms of ML/TF risk are the following:

    a. Not Accepted (business relationship cannot commence or continue)

b. High Risk (enhanced due diligence measures are applied with the regular review taking place at least annually)

c. Significant Risk (enhanced due diligence measures are applied with the regular review taking place at least every two years)

d. Moderate Risk (normal due diligence measures are applied with the review taking place at least every 3 years)

e. Low Risk (simplified due diligence measures are applied with the review taking place at least every 6 years).

6. The classification of customers is determined through a dynamic internal risk assessment scorecard, which is developed in alignment with the regulatory AML/CFT framework and incorporates multiple risk factors, including the source and origin of funds, customer profile, industry, jurisdiction, and other relevant indicators. This classification guides the level of due diligence and ongoing monitoring applied throughout the customer relationship lifecycle. To take reasonable steps, in accordance with the proportionality principle, to ensure that an effective monitoring system is in place that meets its needs and is capable of detecting unusual activity. This includes the implementation of specialised software packages for the continuous monitoring of the customers' accounts, to enable suspicious transactions to be recognised and to maintain procedures for the reporting of such transactions to the appropriate authorities.
7. Adhere to directives and guidance from regulatory and other authorities relevant to sanctions and embargos and ensure strict adherence to BoC´s Sanctions Policy.
8. Cooperate with authorities and other financial institutions to the extent that this is permitted by applicable laws.
9. Adhere (i) to certain requirements of the Patriot Act related to BoC's obligations as a responded bank, as well as (ii) certain requirements of the Patriot Act pertaining to the operation of correspondent banks in the USA which can be applied by overseas financial institutions as well.
10. Ensure that the implementation of the policies, procedures, and controls does not result in a general refusal or termination of business relationships with entire categories of customers who present a higher risk of money laundering and terrorist financing. The risks associated with a specific category of customers are distinguished between the risks associated with individual customers belonging to that category.

BoC no longer relies on Professional Intermediaries (PIs) (i.e., Introducers) for the purpose of the introduction of clients and does not maintain such agreements. In very exceptional cases, BoC could enter into a specific agreement with certain professionals, for services like certification of KYC documents and where the relevant professional has common clients with BoC. Such exceptional agreements, which fall under the definition of "Approved Introducer" of the relevant CBC AML Directive, are approved by the AMLCO, in conformity with the Directive, while the Audit Committee is requested to provide its approval.

BoC is committed to complying with the relevant AML/CTF Laws, Regulations and Directives to maintain the highest possible standards and practices and demands that all management and staff to adhere to these practices.

4.2 Organizational Structure

Each regulated subsidiary appoints its own AMLCO to ensure adherence to the legal and regulatory requirements. The appointment is approved by the Chief Compliance Officer.

BoC's AMLCO is the coordinator for ensuring adherence to the legal and regulatory framework of all entities within BoC and reports to the Chief Compliance Officer.

The AMLCO operates as an independent second line of defense, has unrestricted access to all necessary information and direct reporting rights to the BoD in case of significant incidents. Within the Compliance Department (for all BoC Entities that such a department is required by the legal and regulatory framework) a unit is responsible for the prevention and suppression of ML/FT and the Head/Manager of this Unit is the designated AMLCO. Subsidiary AMLCOs have a direct reporting line to the Audit Committee of the BoC Entity, and a functional reporting line to the Chief Compliance Officer.
Where there is no requirement for a Compliance Department it is ensured that the subsidiary AMLCO has adequate resources for carrying out his/her duties.

Depending on the size of each regulated subsidiary the Head / Manager of Compliance could be the same person as the AMLCO. Where the size of the regulated subsidiary does not justify the creation of a separate Compliance Unit, the role of AMLCO is assigned to a senior staff member independent of the business functions.

4.3 Retention of Records

BoC states all Retention Periods according to Data Type in the Information Security Standard 002 – Data Retention.

4.4 Training

Each Group Entity provides, on an annual basis, adequate and continuous training to all relevant staff members to familiarize staff with the procedures set out in the relevant manuals which are issued by the local Compliance Units of BoC and to enable staff to recognize and handle transactions and activities suspected to be related with money laundering or terrorist financing activities. Also, it encourages staff to make a positive contribution to the fight against crime by reporting circumstances where they become aware or suspicious of any transactions or customers that might be using BoC to launder money.

Compliance senior managers receive regular external specialised training and participate at international compliance conferences / forums.

4.5 Group-Wide Information Sharing

All Group entities may provide information concerning common customers and activities for cases related to ML/TF and respond to requests for account information from other Group entities in a timely manner. This exchange of information is performed by the respective AMLCOs, under the supervision and the coordination of the BoC's AMLCO.

BoC's Group–wide policies and procedures consider issues and obligations related to local data protection and privacy laws and regulations. All information shared between Group entities / subsidiaries is done in compliance with relevant laws and regulations and is provided from / to the compliance functions of each Group Entity.

4.6 Complex Structures and non-standard or non-transparent activities within BoC's own structure

BoC avoids setting up complex and potentially non-transparent structures.

BoC considers in its decision-making the results of a risk assessment performed to identify whether such structures could be used for a purpose connected with ML or other financial crimes and the respective controls and legal framework in place. Therefore, it takes into account at least:

1. the extent to which the jurisdiction in which the structure is set up complies effectively with EU and international standards on tax transparency, AML/CTF.
2. the extent to which the structure serves an obvious economic and lawful purpose.
3. the extent to which the structure could be used to hide the identity of the ultimate beneficial owner.
4. whether the structure might impede appropriate oversight by BoC's senior management or BoC's ability to manage the related risk. and
5. whether the structure poses obstacles to effective supervision by the competent authority.

In any case, BoC does not set up opaque or unnecessarily complex structures which have no clear economic rationale or legal purpose or if it is concerned that these structures might be used for a purpose connected with financial crime.

When setting up such structures, the senior management has a clear understanding of their nature, their purpose as well as the risks associated with them and ensure that the internal control functions are appropriately and timely engaged. Such structures are approved by the senior management of BoC.

5. GOVERNACE

The Roles and Responsibilities within the content of this policy are as follows:

Role	Final
Board of Directors	• Approves the Policy • Bears the ultimate responsibility for the effective implementation of this Policy and for setting the right tone from the top.
Audit Committee	• Recommends the Policy for approval (to the Board of Directors). • Makes sure that sufficient, dependable, and secure internal procedures are in place to ensure that the Group complies with the policy. • Monitors the effective implementation of the Policy via the Control Functions.
ExCo	• Reviews the Policy prior to submission to the AC. • Bears the ultimate responsibility for ensuring compliance with the Law, the Directives and Circulars of the Central Bank of Cyprus, the provisions of Regulation (EU) 2015/847 (Transfer of Funds), and the Guidelines of the EBA.

	• Ensures the introduction and implementation of appropriate and effective internal control systems and procedures, which reduce the risk of the Bank's products and services being used in connection with money laundering from illegal activities and the financing of terrorism. • Ensures that it is effectively embedded throughout the Group's operations.
Compliance Division	• Overall responsibility for the drafting and enforcing the policy. • Prepares and updates relevant procedures/circulars as required. • Organizes and conducts relevant training for all staff. • Carries out monitoring reviews to assess the effective implementation of the Policy and recommends corrective action where required.
Risk Management Division	• Reviews and assesses the compliance risks addressed in the policy, ensuring that the risks undertaken are within BoC's risk appetite.
Internal Audit Division	• Responsible for providing independent and objective assurance to the BoD, through the AC, and to management, by assessing the effectiveness of governance, risk management, and control processes related to this policy. • Informs AC of its findings and relevant recommendations.

6. EXCEPTION APPROVAL PROCESS

Not applicable.

7. IMPLEMENTATION PROCEDURES (KEY PROCESSES)

The BoC Group has in place written, well documented and detailed procedures for the implementation and monitoring of this policy and the policy is effectively communicated to all relevant staff to mitigate any resulting compliance risks.

The procedure also acts as an internal alert and:

1. Provides guidance as to the necessary information to help examine/assess a case.
2. Ensures that the potential or actual breaches raised are assessed and escalated in a timely manner.
3. Ensures the tracking of the outcome and monitoring of mitigation actions.
4. Ensures appropriate record keeping.

Systems and processes are adjusted accordingly, and staff is adequately trained to support effective implementation and monitoring of the compliance with this policy**.**