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

1. PURPOSE

The Bank 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 the Bank 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 at fault.

The Bank examines its AML/CTF strategies, policies, procedures, and programs on an ongoing basis and retains an effective AML program for the Bank's business ensuring compliance with all applicable legal and regulatory requirements. Furthermore, additional regulations on specific issues may be set by the Bank, 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 the Bank'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 the Bank'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 the Bank's reputation by protecting the Bank 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 the Bank.

2. ABBREVIATIONS

Within this document, the following abbreviations are used:

Abbreviation	Definition
AML	Anti-money Laundering
AMLCO	Anti-Money Laundering Compliance Officer
CBC	Central Bank of Cyprus
CTF	Combating Terrorism Financing
FC&SCD	Financial Crime & Sanctions Compliance Department
FIU	Financial Intelligence Unit
ICAAP	Internal Capital Adequacy Assessment Process
KYC	Know Your Customer

Abbreviation	Definition
KYCB	Know Your Customer's Business
ML / TF	Money Laundering / Terrorism Financing
RCSA	Risk and Control Self-Assessment

3. DEFINITION OF TERMS

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

   The term KYC goes beyond the simple identification process, such as the identity card. It is the Due Diligence process that the Bank 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 the Bank's Customer Acceptance Policy, the Bank recognizes that the evaluation of a customer's risk is fundamental in the Bank's effort to prevent and suppress money laundering, terrorist financing and other illegal activities. Hence, the Bank has defined:

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

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

      iii. a list of people classified as High-Risk Customers (physical and/or legal) in accordance with the requirements of the Central Bank AML Directive. For those people 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 must be terminated.

   The Bank has also developed 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 5th 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 will 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). At this stage, 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 through the use of the Bank'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**

   Is 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. Money Laundering is also involved 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. The Bank 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 the Bank which falls under the definition of an "obliged entity" under the Cyprus AML Law
4. **Terrorist finance**
   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. ENTITIES AFFECTED

The Bank of Cyprus ensures that the legal and regulatory requirements emanated from the provisions set out in the Law 188(I) 2007, the 5th 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 the Bank, including its subsidiary companies.

All Bank subsidiaries 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 the Bank, in accordance with established reporting lines.

5. GENERAL PRINCIPLES

5.1 General Principles

All Bank of Cyprus entities must comply with the following Bank's general AML/CTF policies, principles and practices:

1. To maintain appropriate manuals on AML/CTF, including detailed procedures and controls for implementing the Bank's AML/CTF policy.
2. To apply a risk-based approach towards ML/TF risks. This includes assessment on:
   a. country risk
   b. product risk
   c. customer risk – legal form
   d. industry risk
   e. transaction risk
   f. distribution channel risk
3. The main categories which the Bank 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, (simplified due diligence measures are applied with the review taking place at least every 6 years).
4. To strictly adhere to the Bank's Customer Acceptance Policy.
5. To apply appropriate Customer Due Diligence by:
   a. ascertaining the identity of the customer before establishing a business relationship or making a one-off transaction
   b. establishing the Ultimate Beneficial Owner of legal entities taking particular care on the identification of the true owners of trusts, foundations, client accounts and other similar entities
   c. building a detailed Economic Profile of the Customer
   d. undertaking Enhanced Due Diligence for High and Significant Risk Customers and transactions
   e. updating the identification data of customers on a regular basis
   f. Detecting suspicious activities/transactions and where appropriate, reporting such activities/transactions to the local FIU.
6. To take reasonable steps, including 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. To adhere to directives and guidance from regulatory and other authorities relevant to sanctions and embargos and ensure strict adherence to the Bank´s Sanctions Policy.
8. To cooperate with authorities and other financial institutions to the extent that this is permitted by applicable laws.
9. To be extremely cautious with regards to the higher risk services (e.g. correspondent banking, private banking business) and implement enhanced procedures and measures in this purpose.
10. To adhere (i) to certain requirements of the Patriot Act related to the Bank'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.

It is noted that the Bank no longer relies on Professional Intermediaries (PIs) (i.e., Introducers) for the purpose of introduction of clients and does not maintain such agreements. In very exceptional cases, the Bank 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 the Bank. Such exceptional agreements, which fall under the definition of "Approved Introducer" of the relevant CBC AML Directive, must be approved by the AMLCO, in conformity with the Directive, while the Audit Committee will also be requested to provide its approval.

The Bank of Cyprus is committed to comply with the relevant AML/CTF Laws, Regulations and Directives to maintain the highest possible standards and practices and demands all management and staff to adhere to these practices.

5.2 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.

The Bank's AMLCO will be the coordinator for ensuring adherence to the legal and regulatory framework of all entities within the Bank and will report to the Chief Compliance Officer.

Within the Compliance Department (for all subsidiaries that such a Department is required by the legal and regulatory framework) a unit must be responsible for the prevention and suppression of ML/FT and the Head of this Unit will be the designated AMLCO. Subsidiary AMLCOs have a direct reporting line to the Audit Committee of the subsidiary, 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 AMLCO. Where the size of the regulated subsidiary does not justify the creation of a separate Compliance Unit, the role of AMLCO should be assigned to a senior staff member independent of the business functions.

5.3 Retention of Records

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

5.4 Training

Each Group Entity provides, on an annual basis, adequate training to all relevant staff members in order to familiarize staff with the procedures set out in the relevant manuals which are issued by the local Compliance Units of the Bank 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 the Bank to launder money.

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

5.5 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 AMLCOs, under the supervision and the coordination of the Bank's AMLCO.

The Bank's Group–wide policies and procedures must take into account issues and obligations related to local data protection and privacy laws and regulations. All information shared between Group entities / subsidiaries must be done in compliance with relevant laws and regulations and be provided from / to the compliance team of each Group Entity.

5.6 Complex Structures and non-standard or non-transparent activities within the Bank's own structure

The Bank shall avoid setting up complex and potentially non-transparent structures.

The Bank shall consider 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 shall take into account at least:

1. the extent to which the jurisdiction in which the structure will be 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 the Bank's senior management or the Bank's ability to manage the related risk. and
5. whether the structure poses obstacles to effective supervision by the competent authority.

In any case, the Bank shall 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 shall have a clear understanding of their nature, their purpose as well as the particular risks associated with them and ensure that the internal control functions are appropriately and timely engaged. Such structures must be approved by the senior management of the Bank.

5.7. Capital Adequacy and Liquidity of the Bank

Capital requirements emanating from ML/TF risks are calculated under the ICAAP exercise within the context of the calculation of Pillar II capital set aside for operational losses. In this respect, scenarios are drafted relating to either Money Laundering, Terrorist Financing or Sanctions Risk and historical data as well as existing mitigating measures are considered to calculate the expected loss in case the scenario crystalizes. Operational losses could be in the form of penalties, loss of business, legal/operational expenses or any other costs relevant to each scenario.

The provisions set out in this policy should be considered when selecting and drafting scenarios for the purposes of calculating capital requirements emanating from ML/TF risks.

In case operational losses are expected to influence cash flows, their impact on the liquidity stress tests and on the different liquidity matrices will be evaluated by Market Risk.

6. GOVERNACE

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

Role	Final
Board of Directors	Bears the ultimate responsibility for the effective implementation of this Policy and for setting the right tone from the top.
Audit Committee	• Approves the Policy

Role	Final
	• 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. • 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 the Bank's risk appetite.
Internal Audit Division	• Periodically assesses the Policy and the Bank's system of internal controls, corporate governance and risk management processes related to the Policy. • Inform AC of its findings and relevant recommendations.

7. EXCEPTION APPROVAL PROCESS

Exceptions are not applicable for this policy.

8. IMPLEMENTATION PROCEDURES (KEY PROCESSES)

The Group must have in place written, well documented and detailed procedures for the implementation and monitoring of this policy and the policy shall effectively be 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 shall be adjusted accordingly, and staff must be adequately trained to support effective implementation and monitoring processes of the policy**.**