Palestine Islamic Bank

Anti–Money Laundering and Terrorism Financing Policy

POL. AMP.AML

Version: 7.0

Document developed and controlled by: Regulation and Work Procedures Department

- **Version Details**

Version Number	Version Issue Date
07	11/01/2024

Regulation and Work Procedures Department: The Department's signature indicates that the Department has planned the procedures and regulations and that the Department confirms that they are in compliance with the operations and procedures adopted at the Bank.

Contents

1. **Definitions**: The following words and phrases shall have the meaning assigned to them below wherever they appear in this document:

Term	Detail
The Bank	Palestine Islamic Bank and all its branches or offices located inside Palestine and/or abroad.
The Board of Directors / Board	The Board of Directors of Palestine Islamic Bank.
Department Director	The Director of the Anti-Money Laundering and Terrorism Financing Department, who is referred to in the Instructions issued by the Palestine Monetary Authority and the "Anti-Money Laundering and Terrorism Financing Director".
Supervisory Authority	For the Bank, the Palestine Monetary Authority (PMA) is considered the supervisory authority.
The Committee	The National Committee for Anti-Money Laundering and Combating Terrorist Financing
The Unit	The Financial Follow-up Unit.
The Law	Decree Law No. (39) of 2022 on Anti-Money Laundering and Terrorism Financing, and its amendments issued as per Decree Law No. (45) of 2022 that was circulated by the PMA according to Circular No. (209/2022).
AML & CFT Policy / The Policy	The Anti-Money Laundering and Terrorism Financing Policy of Palestine Islamic Bank and its annexes.
Due Diligence	The process of identifying the Customer's identity, his legal status, activities, source of funds, the purpose of the business relationship and its nature, and the beneficial owner (if any), and verifying the aforementioned information, as well as the continuous follow-up of the transactions that are conducted within the framework of the ongoing business relation using any of the tools defined in the relevant regulations, as well as identifying the nature of the future relationship between the Bank and the customer, and its purpose.
Know Your Customer (KYC)	The process of obtaining the sufficient and necessary data required to identify the Customer as required by the Bank according to the terms of

	this Policy. This rule is deemed an integral part of the Due Diligence process and imperative for its achievement.
Business Relationship	The relationship established between the Customer and the Bank in relation to the banking activities and services that the Bank offers to its customers.
Customer	A person connected to the Bank through a business relation, whether this person is a natural person or a legal entity.
Walk-in customer	A Customer who is not connected to the Bank through an ongoing business relationship.
Notification Officer	The Branch and/or Office Manager, or whomever he delegates.
Predicate Offense	Any crime that is committed and results in the production of unlawful funds and the committer of the crime seeks to legitimize such unlawful funds. These crimes are defined as any crime that is specified in the penal law in force or any other law in force in the State of Palestine.
Shell bank	A bank that does not have a permanent place of business in which it receives its customers, does not employ a person or more to perform its activities and actual administrative duties, does not keep records of its transactions and is not subject to inspection by any competent supervisory or control authority, whether in its country of incorporation or any other country, and the presence of a local representative or low managerial level employees shall not be deemed proof of existence for such banks.
Politically Exposed Person	A person, along with his family and relatives, associated persons and partner, who occupies or had occupied a high political or public office position, whether in Palestine or abroad, including political party leaders, judges, legislative council members, prosecutors, heads of state-owned enterprises, heads of institutions, bodies, charities and NGOs, or authorities of the State of Palestine or of any oy other state and the heads and representatives of international organizations, including the board members of such organizations, members of the management and their deputies, or those with equivalent positions.
Electronic Transfer / e-Transfer	Any transfer performed through a bank via electronic means on behalf of the sender, though which funds are sent to another bank where the

	receiver may receive them, regardless of whether the transferor and the transferee are the same person or not.
The Committee Enforcing the Resolutions of the UN Security Council	The Committee established in implementation of Decree Law No. (14) of 2022. The Committee is responsible for implementing the resolutions of the United Nations Security Council regarding combating the financing of terrorism and the proliferation of weapons of mass destruction
Approved Bank Lists	The lists of penalties used by Palestine Islamic Bank, whereby the Bank does not provide any services, nor does it enter into any business relationship with any persons listed therein (natural person or legal entity). These lists include lists obtained through external provider including EU, UN and OFAC lists.
Numbered Account	The account opened under a certain secret number between the Customer and the Bank with the Customer's name only mentioned at the time of opening the account only, whereas all his transactions with the Bank will be made using this number only, without the need to mention his name.
Legal Arrangement	Direct trust funds or any other similar legal arrangements.
Trust Fund	The legal relationship that is established between people who are alive or upon death, through another person or trustee, when the funds are placed under the control of the trustee for the benefit of a beneficiary or for a specific purpose, where such assets form independent funds and not part of the funds of the trustee. The right to the assets of the trust shall remain in the name of the trustee or in the name of another person on his behalf, who shall have the authority to manage, use and dispose of the assets in accordance with the condition of the trust and the special duties imposed upon him by law and the powers conferred upon him.
Direct Trust Funds	A fund expressly established by the testator or person, usually in the form of a document such as a written trust deed, that differs from trusts that are created by law enforcement and do not result from the testator or person's express intent or decision to establish a trust or similar legal arrangements such as Judicially established trust funds.

Virtual Assets	A digital representation of the value that can be traded or digitally transferred, and can be used for payment or investment purposes. Virtual assets do not include the digital representation of official currencies, securities, and other financial assets covered by the Decree Law.
The Beneficial Owner	The natural person who has final ownership or ultimate effective control over a Customer and/or the account of the person he has acted on behalf of. This includes the person who exercises ultimate effective control over a Legal Arrangement or legal person and its management.

2. **Scope of Implementation**:

This Policy shall apply to all Bank activities and services, including Western Union money transfer services. Each party within the Bank shall be held fully liable for enforcing the procedures relating to him. Disciplinary procedures specified in the Personnel Affairs Policy will be applied to all parties who to fail commit to the provisions of this Policy.

3. **Purpose of the Policy**:

This Policy sets forth the general instructions specific to each aspect of the Anti-Money Laundering and Terrorism Financing program in an effort to establish an effective program that is able to protect the Bank from the dangers of Money Laundering and Financing of Terrorism or reduce the possibility of their occurrence. Furthermore, this Policy aims to ensure the compliance of the Bank, its internal policies and work processes regarding all bank services with the Law, instructions and best banking practices issued by local and foreign supervisory authorities, as this will actively participate in the local and international efforts spent in combating the crimes of money laundering and terrorism financing, keeping in mind that failing in this sector will expose the Bank to various risks that might include reputation risks, legal risks and supervisory risks.

4. **Review and Amendment**:

This Policy shall be revised and amended as per the Bank's vision, and in accordance with the business requirements and necessities, and/or in compliance with any instructions and binding laws. In such cases, the updated Policy shall be approved in accordance with the approved approval mechanisms at the Bank and in accordance with the Bank's approved authority matrix.

5. **Exceptions**:

There are no exceptions to this Policy, as it applies to all administrative levels at the Bank.

6. General Policy:

6.1 Introduction:

Pursuant to the Law, and Presidential Decree No. (14) of 2022 on the Enforcement of Security Council Resolutions, and the instructions and generalizations issued by the PMA for the fulfillment of the Law, it is mandatory for all banks operating in Palestine to take all necessary procedures and measures to comply with the requirements of these decisions. One of the most important measures to be met is to develop a general policy or amend the already existing policies so that they reflect all new requirements. In implementation of these requirements, this Policy was developed and will be continuously reviewed to reflect any necessary amendments to comply with the requirements of the Committee, international practices and any other amendments required by the nature of work and does not contradict the Law and any instructions issued thereunder.

6.1.1 Definition of the Money Laundering Crime:

1. According to Article (5) of the Law, a person who commits any the following actions is considered a committer of the money laundering crime:
    a. Exchanging, converting or transmitting funds by any person with that person's prior knowledge that such funds are the proceeds of a crime so as to conceal or disguise the unlawful source of such funds, or to assist a person involved in a Predicate Offence to escape from the legal consequences of his acts.
    b. Concealing or disguising the true nature, source, location, disposition, movement, ownership or rights related to the funds by any person with the knowledge that such funds are the proceeds of a crime.
    c. A person's ownership, possession or use of funds with the knowledge at the time of receipt of such funds that they are the proceeds of a crime, for the purpose of concealing or disguising the unlawful source of such funds.
    d. Participating in, aiding, abetting, conspiring, providing counsel to, facilitating, colluding, concealing or attempting to commit any of the acts provided for under this article.
2. Knowledge, intent, or aim-given that they are basic elements necessary for the offence shall be inferred from factual, objective circumstances to approve the concealed source of proceeds without the need to obtain evidence of the predicate offence.
3. A person is considered to have committed a money laundering crime upon the commitment of any of the predicate crimes, whether such crimes are committed inside the Country or outside of it, provided that such action is deemed a predicate crime

according to the law in force in the country in which such crime was committed and in the State.

4. The crime of money laundering applies to persons who commit the predicate crime. Punishment of the perpetrators of the predicate crime does not relieve them from being punished for the crime of money laundering.

6.1.2 Definition of the Terrorism Financing Crime:

1. A committer of a terrorism financing crime is any person who willfully provides or attempts by any means, indirectly or indirectly, to provide or collect funds, from lawful or unlawful sources, for the purpose of using it, or with the knowledge that it will be used partially or fully for terrorist acts, a terrorist organization, terrorist association or group, or to commit any act of terrorism.
2. A committer of a terrorism financing crime is any person who willfully provides or attempts by any means, indirectly or indirectly, or collects funds from lawful or unlawful sources to enable members to travel to a country other than their country of residence or nationality for the purpose of committing, planning, participating in, preparing or facilitating terrorist acts, or providing or receiving training in terrorist acts.
3. Moreover, a committer of a terrorism financing crime is any person who:
    - Attempts to commit a terrorism financing crime.
    - Acts as an accomplice in any terrorist financing crime or attempts to commit it.
    - Organizes terrorist crimes or directs others to commit or attempt to commit them.
    - Contributes to committing or attempting to commit one or more terrorist financing crimes with a group of persons working for a common purpose.
4. Has knowledge or intent, as essential elements necessary for the crime stipulated in this Article, extracted from factual and objective circumstances.
5. The crime of terrorism financing applies even if the terrorist act did not occur, or the funds were not actually used to implement or attempt to implement it, or the funds were not linked to a specific terrorist act.
6. The crime of terrorism financing applies regardless of the country in which the person alleged to have committed the crime is located, whether in the same country in which the terrorist or terrorist organization is located or in another country, and whatever country in which the terrorist act occurred or will take place.

6.1.3 Penalties Stated in the Law:

6.1.3.1 Penalties for the Money Laundering Offense:

- According to Article (52) of the Law, and without prejudice to any more severe penalty provided for in the Penal Code or any other law, a person who commits the crime of Money Laundering shall be punished by imprisonment for a period of no less than three years and no more than seven years, and a fine of no less than the value of the funds subject of the crime and does not exceed double that value.
- According to Article (53) of the Law, the court shall exempt from the penalty prescribed in this Decree Law any committer who hastened to inform the Unit or any other competent authority of the crime of money laundering or terrorist financing before becoming aware of it. In case the reporting of the crime occurs after the knowledge of the crime, the exemption from the penalty shall be granted only in case the reporting of the crime helps in arresting the remaining offenders or seizing the funds that are the subject of the crime. If a person commits the crime of Money Laundering stemming from a Predicate Offence that constitutes a misdemeanor, the person shall be punished by imprisonment for no less than one year and no more than (3) years, and a fine of no less than the value of the funds subject of the crime.

6.1.3.2 Penalties Imposed on Legal Entities:

- A legal entity that commits the crime of Money Laundering or Terrorism Financing shall be penalized, without prejudice to the liability of any subordinate natural person, with a fine of no less than (10000) ten thousand Jordanian Dinars, and no more than (200000) two hundred thousand Jordanian Dinars or its equivalent in currencies that are legally in circulation.
- The person responsible of the actual management of the violating legal entity, any of the members of its board of directors, or officers, shall be penalized with the statutory penalty set forth Articles (52) and (57) of the Law, if it was evident that he had prior knowledge of the crime or if the crime occurred as a result of a breach of his work duties.
- A legal entity shall be jointly liable for payment of adjudicated fines and remedies if the crime that occurred in violation of the provisions of the Decree Law was committed by an employee working on its behalf and for its benefit.

6.1.3.3 Penalties for the Terrorism Financing Offense:

According to Article (57) of the Law, the crime of Terrorism Financing shall be subject to the following penalties:

1. Without prejudice to any more severe penalty provided for in any other law, any person who has committed or attempted to commit the crime of Terrorism Financing will be punished by imprisonment for a period of no less than (3) years and no more than (15) years, and a fine of no less than (50000) fifty thousand Jordanian Dinars and no more than (100000) one hundred thousand Jordanian Dinars, or its equivalent in currencies that are legally in circulation, in addition to confiscating all mediums used or intended to be used in the crime.
2. Any partner, intervener or abettor in the crime will receive a punishment equal to that imposed on the primary perpetrator.

6.1.3.4 Administrative Penalties:

According to Article (58) of the Law, the administrative penalties shall be as follows:

1. Without prejudice to any specific measures stipulated in any of the other laws, the supervisory authority, when revealing any breach committed by a financial institutions, designated non-financial businesses and professions, or non-profit organizations to the provisions of this Decree Law or any regulations or instructions issued pursuant thereto, or based on the referrals received from the Unit or the competent authorities, has the right to take the procedures or measures described below and impose one or more of the penalties stipulated in this article according to its assessment of the seriousness of the breach:
   - Issue a warning requesting compliance with specific instructions.
   - Request submission of periodic reports by financial institutions, non-financial businesses and professions, and non-profit organizations, on the measures implemented or that such reports indicate compliance with the specified warning.
   - Issue written warnings.
   - Impose a fine of no less than (1000) one thousand Jordanian Dinars and no more than (300000) three hundred thousand Jordanian Dinars or its equivalent in legally circulated currencies, for each violation.
   - Prevent the violator from working in the sectors over which the supervising authorities have the power to supervise and control, for a period to be determined by the supervising authority.
   - Replace or limit the powers of directors, officers, or controlling owners of the entity, including the appointment of a special manager.
   - Stop, suspend, or restrict the practice of work or profession.
   - Withdrawal of a license.

2. For the purpose of informing the public, information regarding the procedures applied in compliance with Clause (1) of this Article may be published.
3. Taking any measure or imposing any penalty stipulated in this Article shall not preclude civil and penal accountability under the provisions of this Decree Law or any other legislation.
4. The supervisory authority shall keep records and statistics related to the administrative penalties and procedures imposed in compliance with the provisions of this Article, and shall provide the Unit with such records when needed or on periodic basis.

6.1.3.5 Penalties for Non-Compliance:

Any person purposely violating the provisions specified in articles (7), (9), (10), (11), (12), (13), (14), (15), (16), (17), (19), (20), (21), (23), (25), (26), (39), (40), (45/2) of the Law shall be punished to imprisonment for a period of no less than three months and no more than two years, or a fine in the amount of no less than (5000) five thousand Jordanian Dinars and no more than (50000) fifty thousand Jordanian Dinars, or its equivalent in any legally circulated currencies, or with these two punishments.

6.1.4 Attachment:

Without prejudice to the provisions of this Decree Law, and the rights of bona fide third parties, and upon a request from the Public Prosecutor, the Court of First Instance or the court competent to hear the case or the competent court that hears the case in the event of its referral, and without prior notification, may decide to place the precautionary attachment, and the decision of attachment shall be subject to appeal.

6.1.4.1 Violation of the Attachment Decision:

Any person who knowingly violates the decisions of attachments issued according to this Decree Law in any manner that includes disposing or trading in the seized funds is considered a committee of a crime and shall be punished by imprisonment for a period of no less than one month and no more than six months, or a fine in the amount of no less than (5000) five thousand Jordanian Dinars and no more than (50000) fifty thousand Jordanian Dinars, or its equivalent in any legally circulated currencies, or with these two punishments, if the committer is a natural person and with a fine of no less than (50000) fifty thousand Jordanian Dinars and no more than (100000) one hundred thousand Jordanian Dinars, or its equivalent in any legally circulated currencies, if the committer is a legal entity.

6.1.5 Suspension of Financial Transactions:

The Unit Manager has the right to order the suspension of any transactions suspected to include the crimes of money laundering or terrorism financing for (3) business days, and the Public Prosecutor, based on the request of the Unit Manager, has the right to extend the suspension period for another period that does not exceed (7) business days.

6.2 Internal Measures for countering Money Laundering and Terrorism Financing:

6.2.1 Anti-Money Laundering and Terrorism Financing Department:

Pursuant to the Instructions of the Palestinian Monetary Authority No. (10 and 11/2019), the Bank has established an independent internal regulatory body under the name the "Anti-Money Laundering and Terrorism Financing Department", managed by the "Director of the Anti-Money Laundering and Terrorism Financing Department". This Department shall have, in compliance with the abovementioned instructions, the following:

- A position on the Bank's organizational structure clarifying its subordination and independence whereby it reports directly to the Board of Directors.
- Independence from any operational activity of the Bank and distance from any responsibilities that may include conflict of interest.
- Easy access to any employee of the Bank, as well as any files, documents, records and internal investigative committees and the necessary tools to enable the effective and neutral performance of its activities including providing systems, programs and authorities which may assist the implementation of its duties.

- Full freedom which enables the Department's director and employees to perform their duties with their own initiative in all of the Bank's sections and departments.
- Freedom to write and submit reports to the Board regarding any violation of the laws, regulations, instructions, or any other violations within the Bank without fear of retaliation or harm by management or any other concerned employee, as well as when informing the Unit of any suspected cases.
- Sufficient resources to allow it to independently, efficiently and effectively perform its responsibilities, including hiring a deputy director and sufficient and appropriate staff qualified in the field of Ant-Money Laundering and Terrorism Financing in line with the Bank's size, transactions and risks it faces.
- A rewards, incentives and salary system for the deputy and staff approved by the appropriate authority at the Bank (Board of Directors).
- Independence from the Compliance Department, the Internal Audit Department or the Risk Management Department in its duties, but its works shall be subject to the audit of the Internal Audit Department, without prejudicing maintaining confidentiality of information related to suspected cases.
- The Department Director will practice full and independent powers in submitting reports on suspicions of Money Laundering or Terrorism Financing acts in any transaction or in replying to the Unit's demands regarding such crimes without being subject to any direct or indirect influence from the Bank's Executive Management.

6.2.1.1 Terminating the Employment of the Director of the Anti-Money Laundering and Terrorism Financing Department:

In case the position of the Director of the Anti-Money Laundering and Terrorism Financing Department becomes vacant for any reason, the PMA must be informed within thirty days, taking into account that termination of the Director's services or his dismissal must be made by a Board decision after discussing the issue with the PMA and clarifying the reasons for such action prior to making the decision.

6.2.1.2 Duties and Responsibilities of the Director of the Anti-Money Laundering and Terrorism Financing Department:

The main duty of the Department Director is to operate as a focal point within the Bank to supervise and oversee all activities related to detecting Money Laundering and Terrorism Financing activities, and to prevent the occurrence of such acts through competent staff and sufficient and effective programs and systems. Additionally, the Director will provide the Bank's upper management with assistance and guidance to ensure effective and efficient management of

Money Laundering and Terrorism Financing risks. The Director will achieve the above through performing the following tasks:

1. Ensure that the Bank fulfills and commits to the requirements and obligations of anti-money laundering and terrorism financing specified in the applicable Law, the instructions issued by the PMA and the National Committee for Anti-Money Laundering and Combating Terrorist Financing and the policies and work procedures adopted by the Bank, including:
    - Taking samples from open accounts and executed transactions and test them for compliance.
    - Submitting reports on anti-money laundering and terrorism financing environment at the Bank and its effectiveness, incidents of failure in implementing AML and CFT procedures, situations where Bank's employees have failed to implement KYC and CDD and the necessary recommendations for addressing and rectifying such issues.
    - Following-up on the immediate implementation of the decisions of the Security Council and the decisions related to suspension of financial transactions issued by the relevant authorities in accordance with the decision of the Committee Enforcing the Resolutions of the UN Security Council, which was formed in accordance with prevailing legislation in the State of Palestine.
    - Retaining internal documents and reports submitted to it as well as those submitted to the PMA and the Financial Follow-Up Unit.
    - Implementing the Risk Based Approach (RBA) and categorizing the Bank's Customers according to their degree of vulnerability to the risks of money laundering and terrorism financing (high, medium, low), taking into account the assessment of the risks targeting the Bank, Customers, products, retails channels and geographical factors.
    - Conducting regular review of the Customer's classification related to the risks of money Laundering and terrorism financing, and in light of any unusual transactions and data and information available to the Bank.
    - Inspecting the Bank's Customer database on the local and international ban and freeze lists in a manner proportional with the size of the database and financial transactions, while documenting the results.
    - Participating in and/or overseeing the preparation of the self-assessment on money laundering and terrorism financing at the Bank, which shall include defining such

risks in reference to the four main axes (Customers, products and services, retail channels, geographical aspect).

- Participating in the assessment of the risks of money laundering and terrorism financing within new products and services and financial and banking technologies prior to releasing them and during the process of their development, in addition to amending previous products, services and technologies, and participating in the implementation of controls and measures required to mitigate such risks and manage them; and documenting the same.

2. Submit recommendations on financial balances, the adequacy of Anti-Money Laundering and Terrorism Financing systems and programs and their need for development and modernization.
3. Respond to requests and enquiries related to financial transitions and money laundering and terrorism financing cases received from relevant bodies in a manner consistent with the laws in force, and to provide these bodies with timely data, records and documents without any delay.
4. Ongoing monitoring and control of financial transactions using the automated systems for anti-money laundering and terrorism financing, as well as overseeing and reviewing all unusual and suspicious financial transactions, and maintain records, studies, and information for the data related to all unusual and suspicious transactions.
5. Receive and inspect all reports received from any of the Bank employees in case such employee suspects that an operation is related to money laundering, terrorism financing, or any Predicate Offences; and to document the results of the same.
6. Notify the Financial Follow-Up Unit immediately of any transactions that might include money laundering, terrorism financing or any Predicate Offences whether such crimes have occurred or are to occur. Suspicion reports must be submitted in accordance with the adopted reporting mechanisms.
7. Inform the Anti-Money Laundering and Terrorism Financing Department at the Palestinian Monetary Authority of suspicious activities and fraud cases that affect the security, safety, and reputation of the Bank.
8. Contribute to the development and implementation of training programs on anti-money laundering and terrorism financing, train Bank employees and inform them on the requirements and developments related to anti-money laundering and terrorism financing in a manner that contributes to reinforcing their ability to detect money laundering and terrorism financing acts.

9. Maintain ongoing contact with the Bank's departments and management to remedy any shortcomings and weaknesses found during the National Risk Audit process that aims at detecting the risks of money laundering and terrorism financing, and ensure that all requirements required for the reinforcement of the AML/CFT environment are available.
10. Provide statistics regarding the following:
    - Number of received information requests and the number of answered requests.
    - Number of suspected cases that were transferred to the Unit according to the type of the suspected crime.
    - Number of reported cases which were archived due to lack of suspicion indicators.
    - Periodicity of checking Customer database against the local and international ban and freeze lists.
    - Number of cases where the Bank's Customer names were similar to the names and entities listed on local and international ban and freeze lists.
    - Training programs and courses provided to the Bank's employees on the updates and requirements of AML/CFT.
    - Number of cases in which currencies, cheques and document were checked due to suspected forgery or fraud.

6.2.2 Roles and Responsibilities of the Board:

1. Establish a specialized internal body for the follow-up on the compliance with the provisions of the Law, which is the Anti-Money Laundering and Terrorism Financing Department.
2. Oversee and monitor the Department and adopt its charter or any official document which the Department is established by virtue of so that the Department has an essential and official status within the Bank.
3. Supervise the work of the Department Director.
4. Adopt a clear organizational structure for the AML/CFT function, and ensure that it is adequate and proportionate to the Bank's size, branches, risk, complication of transactions and Customer database.
5. Adopt job descriptions for anti-money laundering and terrorism financing functions which include the roles, responsibilities, qualifications and traits of the persons filling such functions.
6. Adopt a risk-based work procedures manual for the AML/CFT function (RBA). The manual must be based on the recommendations of the Financial Action Task Force (FATF), international best practices, relevant core principles and guidance issued by the Basel Committee on Effective Banking Supervision. The work procedures manual must clearly determine the function's priorities and responsibilities, work methods and mechanisms for

submitting reports and presenting job results including the mechanism for taking corrective action if any violations are discovered.

7. Ensure the independence of the function and no-interference from other functions, and adopt a clear benefits, incentives and accountability system for AML/CFT function employees at the Bank to be applied in cases of negligence or breach of duties and responsibilities.
8. Provide sufficient budgets to ensure such functions operate in a manner that achieves the purpose of their creation and improves employees' ability to manage and mitigate money laundering and terrorism financing of risks. This shall especially include budgets for training, providing qualified staff and automatic AML/CFT systems and programs and inquiring on international and local ban and freeze lists.
9. Adopt the Policy and the work procedures issued thereunder, and explain to the relevant parties within the Bank the importance of implementing the Policy and the work procedures.
10. Oversee and follow-up on the implementation of this Policy whether directly or through the Review and Audit Committee.
11. Take necessary measures to strengthen the values of integrity, work ethics and professionalism within the Bank, due to these values importance in perceiving laws and regulations as mandatory rules that must be abided by.
12. Verify polarized shareholders by looking into the source of funds and ensuring that the individuals are listed on any lists adopted by the Bank in compliance with the instructions of the National Anti-Money Laundering and Combating the Financing of Terrorism Committee and the requirements of maintaining correspondence with required internal and external bodies if the need may arise.
13. The establishment of the Department shall not repeal or conflict with the responsibilities of the Board of Directors to abide by any laws, regulations, instructions, principles and AML and CFT good practice standards.

6.2.3 Roles and Responsibilities of the Executive Management:

1. Oversee the proper implementation of internal policies and procedures.
2. Ensure that the Bank's internal AML/CFT systems are able to mitigate and deal with money laundering and terrorism financing risks.
3. Circulate the Bank's AML/CFT Policy to all departments and employees of the Bank. In case an employee witnesses any violation to the laws and instructions related to AML/CFT, the employee must inform the Department of such violation immediately.

4. Monitor and audit the Bank employees' accounts to ensure that they are not being misused for the benefit of others and/or in a manner conflicting with their nature or purpose or for criminal activities. Furthermore, the Executive Management must follow up on any employee's unusual financial activities, and check the extent to which such activities are proportionate to the nature of the accounts and monthly income, work to investigate the safety of transactions and sufficiency of due diligence procedures in that regard where such task shall be carried out by one of the supervisory bodies or whomever the General Manager authorizes to do the same, or whomever is acting in his behalf.
5. Enhancing the process of taking administrative and disciplinary measures against violating employees who are proven to have committed events that harm the integrity and reputation of the Bank as a result of misusing their accounts or committing financial crimes such as fraud and embezzlement.
6. Provide the Department with sufficient resources and powers that enables it to properly implement the tasks assigned to it.
7. Comply with the applicable laws and regulations in the field of AML/CFT and any instructions and internal and external circulars issued thereunder as applicable.
8. Provide support and assistance to the Department and cooperate with it on all efforts exerted to protect the Bank from money laundering and terrorism financing acts.
9. Reflect the adopted AML/CFT work procedures onto the applicable work procedures when providing any banking services and ensure that managers and employees understand these procedures.
10. Establishing the Department does not revoke or contradict with the Executive Management and employees' responsibilities to abide by laws, regulations, instructions, behavior principles and standards for good professional practice related to AML/CFT.

6.2.4 Roles and Responsibilities of the Internal Audit Function:

1. Ensure the sufficiency and adequacy of AML and CFT action programs' policies and procedures.
2. Apply Due Diligence procedures and examine the extent of focus on high risk Customers and transactions.
3. Measure the extent of adequate implementation of the Risk Based Approach.
4. Measure the effectiveness of Bank's employees at implementing policies and procedures.
5. Check the adequacy and effectiveness the standards and scenarios defined on banking programs and systems including their ability to determine risks, unusual activities and suspicious cases.

6. Check the adequacy of the record retention procedures and the process of providing relevant statistics.
7. Measure the extent to which the Bank has remedied any shortcomings discovered during previous auditing process.

6.2.5 Automated Systems and Programs:

Automated system and programs are considered one of the most important tools that must be provided to the Liaison Officer to allow him to carry out his tasks properly and in a manner that ensures limiting and mitigating the risks of money laundering and terrorism financing as much as possible. This is achieved by providing the Liaison Officer with the required data and information in a timely manner and with the least amount of effort, as these systems must be interconnected from the moment of opening an account, and includes search activities, inquiries, verification, execution of financial transactions and building a database that provides the following, at minimum:

1. Classify Customers according to their degree of risk while providing indicators regarding changes that occur on the Customers' degree of risk and connect Customers' classification with the size and nature of their transactions.
2. Provide data on Customers, degrees of risk, products, services and periodicity of transactions.
3. Deal with large and complicated transactions and follow up on them.
4. Check Customers' databases for any changes that occur to a Customers' classification on international ban lists.
5. Periodically enquire about Customer database on international and local ban and freeze lists and enquire about the parties to external and financial transactions prior to executing them.
6. Oversee Customers' financial transactions, their relationship with the beneficiaries from those transactions and any changes to the nature and size of transactions.
7. Provide indicators regarding any notes suspicious activity requiring monitoring, tracing and analysis to prevent the occurrence of a money laundering and terrorism financing acts, and provide indicators and parameters to monitor transactions and provide a basis for classifying some transactions as unusual transactions.
8. Extract sufficient and accurate information regarding the changes in the nature and size of usual transactions and Customers' degree of risk, oversee financial transactions and provide warning indicators to monitor transactions according to several scenarios.

9. Provide adequate powers to AML/CFT Officer to use the available systems and programs to monitor, follow up and oversee transactions and to the extent which allows him to benefit from the system's outputs, extract necessary report for supervision and follow up on the level of transactions, accounts and Customers.
10. Flexibility and ability to update and develop in a manner that serves the methodology and framework of AML/CFT activities.
11. Extract control report and submit them to supervisory authorities and the Bank's management. Such reports shall be extracted on three levels (transactions, account, Customer) as follows:
    - **Transactions Level**: Money transactions and incoming and outgoing cash flows according to the country, occasional and unusual transactions according to the associated level of risk and certain limits and sizes, large deposits and withdrawals, transactions that were rejected due to the associated risks, the purpose for opening the account, early payment of facilitation balances, divided and collective transaction, reports on transactions performed on accounts of non-profit organizations.
    - **Account Level**: Account turnover rate (debt and credit transactions), cash average (deposit/withdrawal) of overall credit and debit transactions, regularity of account turnover, regularity of loan payment, regularity of account updating, account feeding sources including accounts related to the account, account uses, Customer related data (foreigner, resident, non-resident, nationality).
    - **Customer Level**: According to a Customer's risk classification, high-risk countries with which financial transactions are exchanged, Customers listed on international and local freeze lists, new Customers, Customers whose degree of risk changed according to certain sectors and segments.

6.3 Risk-Based Approach (RBA):

Adopting a risk-based approach has become a mandatory requirement as per the provisions of the Law and the recommendations of FATF. This method, if drafted and built in an effective and correct manner, will assist in protecting the Bank from the risks of money laundering and terrorism financing, or mitigating such risks to the largest extent possible. To achieve this, the needed efforts must be exerted to determine the risks of money laundering and terrorism financing and allocate the necessary resources to control and prevent such risks which will allow more effective use and allocation of resources available to the Bank by prioritizing larger risks.

Based on the requirements of the PMA, the Bank must assess the risks of money laundering and terrorism financing for its vitality in adopting the risk-based approach in the control process, which includes developing the Customer risks classification matrix. Furthermore, the Bank must monitor all daily transactions performed on the Customers' accounts through the different distribution channels, taking into account that the self-assessment process is based on the below specified risk factors:

6.3.1 Customer-Related Risks:

Money laundering and terrorism financing risks that may arise depending on the nature of the Customer's activity and risks inherent in such activity. Accordingly, Customers may be categorized based on the degree of risk included in the nature of their work and activity.

Some Customers may be considered low-risk customers; these include individuals (natural persons) working in jobs with a relatively stable income, or even companies (legal entities) with good and well-known reputation throughout the country and which has an old and documented history proving its source of income and nature of its activity.

Other Customers may be considered high-risk whether they are natural persons, such as PEP, legal entities such as charities, non-governmental organizations and non-profit companies.

6.3.2 Products and Services Related Risks:

Product and service related risks vary according to how the products and services may be exploited by money launderers and funders of terrorism. For instance, services which provide secrecy such as safe deposit boxes and electronic services are of high risk compared to other services provided by the Bank. Consequently, it is possible to classify Customers based on the degree of risk associated with the services that they request.

Indicators of high risk include: services which in their nature allow for the concealment of true identity or using aliases and services or products which allow collecting Customer's funds within containers.

6.3.3 Country or Geographical Area Related Risks:

Resident Customers or Customers who are connected to high-risk countries are considered high-risk customers. These countries include:

- Countries or geographical locations specified by FATF as countries with strategic shortcomings in AMT/CFT or as uncooperative counties.
- Countries or areas under sanctions or similar procedures imposed by the UN Security Council.
- Countries that are highly exposed to corruption.
- Countries which are strongly believed to be related with terrorist activities.

- Countries that are considered as high-risk countries by the National AML and CFT Committee according to Paragraph (16) of Article (20) of the Law.

6.3.4 Distribution and Delivery Channels-Related Risks:

Channels through which services are ordered or delivered to the Customer affects the risk profile for that Customer, especially in cases where the banking services are requested or offered through means that allow for the absence of physical presence, such as email, expedite mail, telephone, and internet banking services.

Based on the four criteria mentioned above, the Bank's Customers have been categorized into various risk levels (high, medium, low). The special annex clarifies these categories, taking into account that there is some flexibility in the listed categories within each classification corresponding to the change in risk levels associated with each category and in line with business requirements. Moreover, for some services, not all beneficiaries are classified as high risk customers, and daily monitoring of these services is considered sufficient. These services will be documented in the relevant annex.

These standards and classifications must be reviewed periodically as part of the Policy for the purpose of applying any amendments if needed, and supervisory and regulatory authorities must be notified of any amendments applied to them.

6.3.5 Self-Assessment of Risks:

1. Regarding the self-assessment of risks process, the Bank shall commit to the below:
   - Update the assessment process on regular basis and whenever needed.
   - Document the assessment process and the updates made to it, and maintain such documents.
   - Provide the Supervisory Authority to the results of the assessment process when it is completed or whenever requested.
   - Circulate the results of the process among all employees and clarify it to them.
2. Based on the results of the self-assessment process for money laundering and terrorist financing risks, a comprehensive methodology was prepared to classify customers' risks based on the four criteria referred to above, noting that this methodology is subject to modification and change based on internal data and local legislation.

6.4 Documents and Records Retention:

1. Electronic Archiving Systems:

The process of retaining documents and records relating to different financial transactions is considered a necessity and a legal requirement. The Bank must provide an electronic archiving

system for records and transactions, which must correspond to the Bank's scope of activities, business size and complexity of its operations, in order to ensure the following:

- Review and follow up on the transfer of funds through the Bank to any Customer or to the Beneficial Owner from the Customer account or the financial transactions.
- The ability to define and identify any Customer or the Beneficial Owner for the Customer.
- Provide all information and records specific to the Customer and transactions in due time, to be provided to the PMA and relevant authorities upon request.
- The Bank's ability to comply with any regulatory, legal or any other requirements imposed by the Law and the instructions issued thereto, including records relevant to a Customer's risk assessment, suspicion reports or records specific to training and employee awareness.

2. **Retention of records related to Customers' identities and transactions**:

1. All management units at the Bank, each according to its competence, must retain, throughout the period of the Business Relationship with the Customer and for a period that does not exceed 10 years from the date of the termination of the relationship, the following documents:
   - The original copy and/or a certified true copy of all documents, information and data records obtained as part of completing due diligence, KYC and verification procedures contained in this Policy and procedures issued thereunder, including information on identifying and verifying the Customer's identity, the Beneficial Owner, the beneficiary, persons representing the Customer in performing transaction on his behalf and/or other parties related to the Customer.
   - Any additional information on the Customer and/or the Beneficial Owner which may be obtained as part of the due diligence procedures or continuous follow-up.
   - The original copy and/or a certified true copy of records, information and data records related to the purpose and the nature of the Business Relationship with the Customer, whenever possible.
   - The original copy and/or a certified true copy of records and documents related to to the Customer's account (for example: account opening form, risk assessment form) and any correspondence with the Customer or Customer's Beneficial Owner (which should include at a minimum those correspondences related to due diligence procedures and any material changes related to the account activities).

2. All administrative units within the Bank must, each according to its own competence, retain the original copy or a copy of the documents and information obtained from completed transactions. Such documents and information should be sufficient and available to prepare a financial profile for each suspected Customer or account. Examples of these records include (the identities of the parties to the transactions, nature and date of the transaction, nature and amount of the transaction, source of funds, method of receiving the funds or withdrawing it such as receiving or withdrawing by cheque or cash, destination of funds, instructions or orders relating to the transaction, account nature and number included in the transaction). These records must be retained for a period of no less than 10 years from the date of transaction completion, the date of the termination of the business relationship or the date of occasional transaction.
3. Competent parties must retain records and documents related to a Customer or financial transactions for a period of more than 10 years if such request was made through a written notice for reasons related to ongoing investigations or any other reason included in such notice.
4. In case there are investigation cases related to money laundering or terrorism financing crimes, the relevant bodies at the Bank must retain documents and records relating to the transaction/Customer subject of such case until the end of the investigation. Having a written notice is not required in this case.

6.5. Customer Identification and Verification Policy

1. Objectives of the Know Your Customer (KYC) Policy:

The Bank's Know Your Customer (KYC) Policy is considered an integral part of its AML/CFT Policy due to the effective role that it has in preventing the Bank from entering into a relationship with a Customer that might expose the Bank to risks resulting from the exploitation of its services and using them to perform money laundering and/or terrorism financing acts. The objectives of the KYC policy are:

- To ensure the Bank's commitment to all international and local laws and regulations in force on AML/CFT.
- To emphasize the importance of applying KYC procedures prior to and after establishing the Business Relationship. Through this process, any information that supports the identification of the customer, nature of his activities, source and size of income and any other information are obtained to help enrich the Bank's information regarding such customer.
- To constantly follow up of the Bank's Customers in order to recognize good customers and seek to retain them.

- To avoid dealing and/or stop dealing with any Customer who refuses to provide the Bank with necessary data and information in accordance with this Policy.

2. Risks Associated with the Failure to Implement the KYC Policy:

Failure to provide clear standards and measure to verify Customer's identities will result in many risks that may lead to the Bank facing financial and moral losses. These risks include reputation, legal and operational risks. Below is a clarification for each of these risks:

1. **Reputation Risks**: Reputation risks result from Customers' and investors mistrust in the Bank due to losses resulting from the downsizing of its operations in the local and international markets or from fines imposed by supervisory authorities.
2. **Legal Risks**: Legal risks result from law suits and legal procedures that might be taken against the Bank due to its relationship with suspicious Customers or Customers involved in money laundering and/or terrorism financing acts.
3. **Operational Risks**: Operational risks result from the fines that may be imposed on the Bank due to its non-compliance with the instructions issued by the Unit or the supervisory authority.

3. Politically Exposed Persons (PEPs)

The Bank must provide adequate systems for risk management that allows it to determine if a Customer or a Beneficial Owner is a politically exposed person; if that is the case, then the following shall be applied:

- Apply the adopted procedures for identifying this type of Customer.
- Obtain approval from the Bank's senior management prior to establishing any relationship with the Customer.
- Take all reasonable measure to know the source of fortune and funds.
- Provide enhanced and ongoing monitoring of the Business Relationship with this Customer.
- Take all reasonable measure to confirm the circumstances of work surrounding any Business Relationships and transactions with PEPs and their purposes. In case it is evident to the Bank that any relationship or transaction do not have clear economic justifications, the Bank must document the result of its procedures in its records.

4. Relationship with Corresponding Banks:

When dealing with corresponding banks, the following measures and procedures prior to the initiation of such relationship, taking into consideration that the Banks is not allowed to enter into any business relationship with what are referred to as virtual banks or Shell Banks:

- Identify and verify the recipient institutions with whom the Bank intends to establish a correspondent relationship.
- Collect information on the activities that the institution carries performs, to understand the nature of the activities that they implement.
- Evaluate the recipient institution's reputation and the nature of supervision it is subject to, based on published information, and to look into whether they have been investigated for money laundering or terrorist financing activities, or if any supervisory or regulatory measures have been taken against them.
- Obtain senior management's approval prior to establishing a correspondent relationship.
- Evaluate the controls adopted by the institution regarding AML/CFT, including the adequacy of business policies and procedures, risk-based approach procedures, availability of systems and programs, and any AML/CFT questionnaires
- Ensure that the recipient institution verifies its customers' identities, implements ongoing monitoring mechanisms on its customers and is able to provide relevant identifying information upon request.
- Clearly understand the responsibilities of each institution in the field of combating money laundering and terrorist financing.

5. **Prohibited Risks**:

Based on the result of the self-assessment process for money laundering and terrorism financing, the Bank can deal with customer, Products and services, as well as geographical areas with high, medium and low risks as specified in the Manual, including all four aspects adopted in the classification process expect what is specified below, as the following risks are considered banned risks on the level of Palestine Islamic Bank:

Customers	
1	Customers listed on the sanctions lists issued by the United Nations Security Council.
2	Customers who are hard to be identified and verified, and the due diligence procedures cannot be applied on them or on their transaction, when establishing the Business Relationship and throughout it.
3	Customers who are suspected to deal or have a relationship with criminal activities based on negative news and trusted independent sources.

4	Customers residing in high-risk countries, or those who perform their activities in such countries, or hold their nationality as the only and main nationality.
5	Customers residing in banned countries, or those who perform their activities in such countries, or hold their nationality as the only one, except Israeli Citizens.
6	Clients who are anonymous or bear fictitious or fictitious names.
7	Shell Companies and Banks.
8	Customers listed on the National and United Nations' Lists or those dealing with listed bodies.
9	Customers who request the delay of identification and verification procedures.
10	Customers who request establishing a Business Relationship through None Face to face method or through a Power of Attorney.
11	Customers residing in Israeli settlements established on the 1967 boarders.
12	Walk-in Customers except those performing cash deposit in a Bank customer account, Wester Union, or check encashment transactions.
13	Customers residing in offshore countries or remote islands (in the list of high-risk countries).
14	Customers who deal with virtual currencies.
15	Customers engaged in financial and investment activities without obtaining the necessary licenses from competent authorities.
16	Legal persons with nominal or nominated shares (Nominees).
17	Legal persons issuing bearer shares (there are no specific owners or the owners change continuously).
Services and Products	
1	Numbered accounts.
2	Payable Through Accounts in corresponding banks relations or PTA.

3	None Face to face account opening requests or requests made through a Power of Attorney.
4	Financial Transactions with financial institutions or any of their branched located in the settlements established on the 1967 boarders.
5	Virtual currencies.
6	Special banking services.
7	Anonymous financial transactions (whether one of its parties is unknown or the source of its funds is unknown).
8	Services that allow payment by unrelated third parties.
9	Traveler's checks.
Geographical Areas	
1	North Korea, Iran, Myanmar, or any updates according to the updates on internal high risk countries' list.

6. Updating Customers' Data

After establishing a Business Relationship with a Customer, the related branch must take practical steps from time to time to ensure that the data acquired from the Customer has not changed, and make any necessary updates in case of changes, whether partial or complete. The following cases are considered instances which the Customer's data must be updated instantly, while noting that the Customer's degree of risk requires more frequent follow up and update:

1. Performing an important transaction. (Keeping in mind that an important transaction does not necessarily refer to the financial value of that transaction, but might also mean that the Customer has performed on the account a transaction that is incompatible with the Bank's knowledge and understanding of the Customer).
2. A fundamental change to the activity on the Customer's account.
3. A material change to the documentation standards of Customer's data.
4. Lack and weakness of the information available about a Customer.
5. When the Customer requests the activation of his account.
6. When the Bank has suspicions regarding the accuracy or appropriateness of the data that was previously obtained regarding the identification of the customer or the adequacy of the provided documents.

7. Detecting any unusual activities on the customer's account.
8. Suspicions of money laundering or terrorism financing crimes, or any of the related crimes.
9. Raise in the customer's risk rating according to the Bank's approved rating methodology.
10. Update the data based on the degree of risk associated with the client annually, every three years, and every five years for high, medium, and low risk clients, respectively.

7. Due Diligence

6.5.7.1 Due Diligence Measures

Due Diligence is an important process for obtaining the required vital data and information to better understand the requested transactions (listed below) and to verify if such transactions include money laundering/ terrorism financing acts. Therefore, the following due diligence procedures must be taken with regards to Customers regardless of their classification (natural person or legal entity) keeping in mind that AML and CFT procedures presented in the approved Manual details the due diligence procedures that must be applied for each type of customer and each service/activity within the Bank:

- Not to maintain any anonymous accounts or accounts under fictitious names.
- Identifying its Customers and verifying their identities using reliable and independent documents, data and information.
- Verify that the person purporting to act on behalf of the client is duly authorized, and identify and verify his or her identity.
- Identify the Beneficial Owner for the transaction and take reasonable measures to verify his identity using documents, information, or data obtained from a reliable and independent source to convince the financial institution that it is aware of the Beneficial Owner.
- Understand the purpose of the work relation and its nature, and collect information about it as needed.
- Understand the nature of the client's work when the client is a legal entity or legal arrangements, and the ownership and administrative hierarchy.
- Carry out continuous due diligence on any business relationship, including carefully studying the operations being carried out and their purpose to ensure that they are consistent with the information in their possession about their clients, their business activities and their risk profile, including if necessary the source of funds, and ensuring that documents, data or information collected pursuant to this Article are constantly updated and appropriate, by reviewing existing records, particularly for high-risk customer categories.

6.5.7.2 Timing of Professional Diligence Procedures:

All administrative units within the bank must apply the professional due diligence measures mentioned above in the following cases, based on what is stated in the Law:

a. Establishing a relationship with the customer.
b. Executing any casual transaction with a value of 15,000 US dollars or above or its equivalent in other currencies, whether it is conducted as a single transaction or several transactions that appear to be linked to each other.
c. Executing occasional financial transactions in the form of internal transfers or wire or electronic transfers inside or outside Palestine, regardless of their value.
d. Having doubts about the validity or adequacy of customer identification data obtained previously regarding customer identification or their adequacy.
e. Suspicion of money laundering or terrorist financing acts.

8. Enhanced Due Diligence (Special Diligence)

Instructions issued by the PMA and the Committee stated the necessity of applying the EDD procedures on all Customers that are classifies as high-risk Customers or for the transactions that are connected to high-risk countries. The applied procedures shall include:

a. Conduct a check on the background and purpose of all unusually large and complex financial transactions and all unusual patterns of financial transactions, which have no clear economic or legal purpose, to the extent possible and in a reasonable way.
b. Obtain additional information about the Customers, such as additional information about the profession, economic activities, other sources of income, the amount of funds or assets, and information available through public databases, the internet, and others sources.
c. Conduct periodic updates of identification information, and verify the customer's information and data based on the customer's level of risk.
d. Obtain additional information on the nature of the Business Relationship intended to be established with the Bank (expected activities).
e. Obtain additional information about the customer's source of wealth and fund, and verify such information.
f. Obtain more information about the purposes and reasons for expected or conducted financial operations.
g. Obtain Senior Management approval regarding initiating a Business Relationship or continuing the same.

h. Increasing control and supervision over the Business Relationship in a manner appropriate with the degree of risk associated with this Business Relationship by increasing the number and timing of the applied control measures.

i. In case a customer has accounts in one of the banks that are subject to due diligence criteria, the first payment can be requested to be made through the customer's accounts at that bank.

9. Terminating the Business Relationship with the Customer (Inability to complete due diligence procedures):

In the following cases, the Bank shall refrain from establishing new relations with new customers, and for existing Customer, the Customers must be notified of the termination of the Business Relationship with him after informing the Financial Follow-up Unit when needed, while taking into consideration the terms of the Law and the Instructions related to the freezing of the funds of Customers listed on the international lists and the lists adopted by the Committee:

- The Customer's refusal to update his data in the cases that require update of data as specified in Clause (6.5.6) of this Policy.
- The Customer's refusal to provide the Bank with the data, documents, and supporting documents required for the completion of the Due Diligence procedures in cases requiring the implementation of such procedures as specified in Clause (6.5.7) of this Section.
- In case the Customer is listed on any of the lists adopted by the Bank or those circulated by the PMA and the Committee.
- In cases of suspected money laundering or terrorist financing acts, and if there are logical and reasonable reasons indicating that conducting due diligence will result in notifying the customer, it is permissible not to continue applying the due diligence measures, and to submit a suspicious transaction report to the Unit.

6.6. Know Your Employee (KYE) Rule:

1. In implementation of the "Know Your Employee" rule, which states the financial institution's obligation to know its employees, their reputation, their behaviors and their source of wealth, as part of ensuring that the employees do not take advantage of their powers in cooperating or complicating with any external parties or performing any activities that might harm the Bank, such as fraud and misuse of trust, therefore, the Human Capital Department must follow the below procedures before hiring Bank employees:
   a. The Human Capital Department must obtain all the data from the candidate's personal identity card.

b. The Human Capital Department must request a Non-conviction Certificate issued by the Ministry of Justice which states that the candidate was not previously convicted with any misdemeanor or felony.

c. The Human Capital Department must investigate the candidate through an inquiry on the cheques system managed by the PMA.

d. The Human Capital Department must check the candidate's name on the lists adopted by the Bank through the Safe Watch program.

e. Knowledge of the private business that the candidate has through a dedicated form. The form must include a pledge by the candidate to disclose any other transactions performed on his account or any amounts deposited in his account other than the salary that he receives in return for his work at the Bank.

f. The above-mentioned form must include a clause related to the disclosure regarding any unpaid or volunteer activities that he performs, such as membership in committees or organizations and volunteer work in any organizations … etc.

g. The employee must sign a pledge to commit to the contents of the Code of Conduct approved by the Board and its annexes, including this Policy.

h. To apply the procedures that mitigate the risks related to services and products, distribution channels, geographical areas and customers on the Bank employees by all parties, each according to its responsibilities.

2. The requirements of the Know Your Employee rule referred to above represent the minimum requirements that must be adhered to, noting that the Executive Management is responsible for formulating the appropriate operational procedures to control the risks associated with employees.

6.7. Procedures related to Contracting with Suppliers and Consultants, and Processing Social Responsibility Requests:

a. Whenever the Administrative Affairs Department wishes to deal with an external party, whether based on its needs or the needs of other departments within the Bank, the Administrative Affairs Department must obtain all data related to the supplier regarding its actual physical existence, its address, as well as checking the names of the supplier on the Safe Watch program before initiating any work with them. Furthermore, monthly inquiries regarding the suppliers should be done throughout the duration of the relationship.

b. All administrative units within the Bank must commit to obtaining all data related to external parties they deal with, including their address, their actual physical

existence, their licenses from the competent authorities, good reputation, as well as checking the names of the supplier on the Safe Watch program.

c. Before providing any assistance or donations to any external party as part of the Bank's social responsibility, it is necessary to inquire about the lists approved by the Bank through the Safe Watch program.

6.8. Reports and Reporting:

a. The Bank shall duly check the background and purpose of all unusually large and complex transactions, and patterns of unusual transactions that have no clear economic or legal objective, to the extent possible, with particular care.

b. The Bank must prepare a written report containing specific information on commercial relations and operations as mentioned in Clause (1) of this Article, and the identity of all concerned parties. This report must be kept, and must also be submitted upon the request of the Unit, the supervising authority, and any other competent authorities.

c. When suspecting that certain funds are the outcomes of a crime, or when the Bank has reasonable justifications for such suspicion, or that such funds are related or connected to a money laundering or terrorism financing act, or if it has knowledge of any instance or activity that indicated a money laundering or terrorism financing crime, or any of the related predicate crimes, then the Bank must immediately submit a report on such incidents to the Unit, as per the related work procedures regulating this issue.

d. The bank shall immediately inform the Unit of all suspicious transactions and activities, including attempts to conduct such operations, regardless of their value.

6.9. Disclosure:

All employees of the Bank are prohibited from disclosing to customers or any third party any information that has been provided to the Unit, or that a report has been filed in relation to a suspected money laundering or terrorist financing crime or a predicate offence, or that such reports are being prepared or will be submitted to the Unit, or that there has been an investigation of money laundering, terrorist financing or any of the predicate offenses or that the such will be conducted

6.10. Training and Qualification:

1. Training and qualification are considered necessary pillars for establishing an effective AML/CFT program. When the staff are not adequately qualified in this field, the effectiveness of the applied Internal Audit System is weakened. Therefore, the Human Resources Department at the Bank, and in coordination with the concerned department, shall develop a training policy which focuses on aspects of AML/CFT. Additionally, sufficient budgets must be allocated for the implementation of such trainings in a manner that serves the Bank's perspective and goals of strengthening its internal environment against risks of money laundering and terrorism financing.
2. All functional levels within the Bank must be targeted in this type of training, including newly hired employees prior to being assigned any of their tasks. Training programs must align with the special needs of each level and area of function, in addition to repeating the trainings to the extent and in a manner that guarantees maintaining the level of knowledge and competence required for employees to perform the tasks assigned to them in a manner that ensures that the Bank, and its employees, are not exploited in any money laundering or terrorism financing acts.
3. All bank Employees must be aware and knowledgeable of the following:
   - The legal responsibilities of the Bank and their personal legal responsibilities, as well as the possible consequences of the failure to report suspicious operations as per the terms of the Law.
   - Any legal obligations of the Bank and its employees according to the terms of the Law and the instructions issued by the Committee, and the possible consequences of breaching such obligations.
   - The Bank's policies and procedures related to AML/CFT, including determining suspicious transactions and reporting them.
   - Any new methods, ways and directions in the field of AML/CFT to the extent that such information is considered necessary for the employees to enable them to perform the tasks assigned to them properly.
4. Employees training must cover the following fields:
   a. For all employees, regardless of their job level:
      - A general introduction to money laundering and terrorism financing activities, and the importance of having systems to counter them within the Bank.
      - The importance of identifying and reporting any suspicious transactions to the Anti-Money Laundering Liaison Officer, and the crime of trying to conceal them.

b. **Employee who directly deal with the public (such as customer service employees, tellers, "Western Union" transfer services employees)**

- The importance of their roles in the Bank's strategy on AML/CFT as the first contact point with potential money launderers.
- Customer due diligence and follow up procedures and the requirement of retaining records relating to the duties imposed on them.
- Circumstances that increase the possibility of suspicious cases and related policies and procedures including, for example, reporting channels and cases which require additional care.
- Fraud indicators which may be discovered with regards to issued and received Western Union transfers, and how to deal with them.

c. **Back Office Employees**:

- Appropriate training in KYC and applicable related procedures.
- How to identify unusual activities including settlements, unusual payments and Customer instructions on the methods of services delivery.

d. **Officers and employees in supervisory departments including officers and employees of internal audit and compliance departments**

- Specialized training in all aspects related to the AML/CFT system at the Bank.
- Specialized training on their responsibilities regarding oversight and supervision of staff, auditing the system and randomly testing it, special training on self-assessment for AML and CFT procedures supervised by the Liaison Officer for the purpose of attaining التكاملية between supervisory roles and the role of the Liaison Officer.

e. **Department Director and Employees (including, but not limited to the below)**

- Special training on their responsibilities in assessing suspicious transaction reports submitted to them, and reporting them to the Financial Follow-Up Unit.
- Training programs that keep up with the developments in AML/CFT requirements.
- Training on patterns and recent applications in AML/CFT systems.

- Training on the above mentioned subjects is done either internally on issues related to internal policies and procedures or externally on issues related to identifying the crimes of money laundering and terrorism financing and developments applied to instructions regulating the efforts to combat this crime locally and internationally.
- Regardless of the training methodology used in providing the trainings, the Training Section in the Human Resources Department shall maintain dedicated records for each performed training meeting with evidence that prove that the approved training plan was duly implemented. These records must include: a list of the employees who attended the training, the nature of their work inside the Bank, training date and training content. These records are deemed sufficient evidence that prove that the training was successfully completed by the Bank.
- Based on the daily communication and interaction between the Department and the other units within the Bank, as well as the results of the internal audit (special or routine audit), the effectiveness of the training programs offered to the employees is measured through several indicators, including for example:

    1. The Efficiency and effectiveness of the Bank's employees in internally reporting and detecting suspicious transactions.
    2. Type of enquiries received by executive units within the Bank.
    3. Notes and results of internal audit checks.

6.11. General Provision and Requirements:

1. Relying on a third party: Palestine Islamic Bank does not rely or depend on any third parties for the implementation of the requirements of professional due diligence or enhanced due diligence.
2. The decisions of the United Nations Security Council: the importance of committing to the contents of the Presidential Decree No. (14) of 2015 regarding the implementation of the Decisions of the United Nations Security Council, whereby specific procedure for checking in advance on the lists adopted by the Bank (UN, EU, OFAC) through the Safe Watch program are put in place as a requirement for accepting Customers or accepting dealing with them, and for each banking service. Additionally, a mechanism to follow-up on all generalizations issued by the PMA and relating to updates on accredited international lists in accordance with the abovementioned Presidential Decree must be defined.
3. Ongoing Follow-up: The Department shall handle the responsibility of continuously following-up on transactions performed on the Customers' accounts through daily reports obtained in cooperation with the Information Technology Department, in addition to the indicators detected using the I-Detect system.
4. Ongoing follow-up by branches: The managers of the branches are responsible for the ongoing follow-up for its Customers' accounts whereby the Department is informed of any suspicious cases according to the defined procedures as part of the "Suspicion and Internal Reporting Manual" issued in accordance to this Policy. Failure to report is considered as a strong indicator of the branch management's failure in implementing AML/CFT procedures.
5. All branches and departments must review the policies and procedures related to AML/CFT and work to implement the relevant procedures that fall within their responsibility and provide the Department with what is required without delay and without the need to refer to the customers.
6. The Marketing Department and the Programs and Products Development Departments shall work to submit the procedures for implementing any new services or modifications to the existing services for review by the Department in order to identify the risks of using these products/services in money laundering and terrorist financing operations and to work towards setting procedures that limit or mitigate these risks.

7. The process of reporting suspicious transactions is considered an integrative process that aims at protecting the Bank from the risks of money laundering and terrorism financing, where each employee with the Palestine Islamic Bank is responsible by virtue of his position for the reporting of any activity that he suspects is related to money laundering and terrorism financing. The Department must be notified of such suspicions using the dedicated form and it shall study the form and take appropriate decision in that regard (further inquiry, close the case, report externally to the Unit).
8. One employee from each branch/office must be assigned as a "Notification Officer".
9. The Bank must implement due diligence and ongoing care in the Business Relationship and must carefully study all performed transactions and their purpose to ensure that they are in-line with the information that the Bank has about its customers, their commercial activities and their risk profile, and when needed, confiscate their funds according to the Law.
10. Not to accept any copies or photocopies of any customer documents without seeing the original documents; after seeing the original documents, the concerned employee shall stamp the copy with a "true to original copy" stamp.
11. Refrain from providing any services to walk-in customers, except for fast money transfer services such as Western Union service.
12. Suspicion indicators must be taken into consideration when dealing with Customers and opening new accounts for them, and that these indicators – whenever they exist – are dealt with according to the terms of the "Suspicion and Internal Reporting Manual".
13. The Programming and Banking Systems Department is responsible for updating the lists of high-risk countries on I-Detect program and Safe Watch program in case any updates are received based on the Generalizations of the PMA and as per the procedures adopted by the Bank.
14. All parties within the Bank must immediately inform the Department of any fraud and/or currency or documents counterfeiting that are detected.
15. The Procedures Matrices that control the risks of money laundering and terrorism financing inherent in services, products, distribution channels, geographic areas, and clients, is an integral part of this Policy, and therefore all parties must assume their responsibilities regarding the implementation of what is stated in it based on the approved and circulated documents by the Regulation and Work Procedures Department.