Ooredoo Palestine

ANTI MONEY LAUNDERING

POLICY

TABLE OF CONTENTS

1.0. Purpose

1.1. The Purpose of the Anti-Money Laundering Policy (Policy) is to assist relevant banks and other financial institutions that are working with the Company to implement OMM to adhere to Laws, Guidelines and Regulations from Central Bank and other statutory requirements on Anti-Money Laundering and combating terrorist financing as per the agreement with the relevant banks.

1.2. To ensure that feasible Anti Money Laundering controls are in place for early and effective identification, detection, prevention and reporting of money laundering, terrorism financing and potential financial crimes.

1.3. To ensure that management systems and processes are in place for early identification of gaps that could lead to financial crime and terrorism financing and subsequently recommend / implement controls for the prevention of such activities.

1.4. AML and Compliance function under Revenue Assurance Department in the Company aims to implement the highest standards of anti-money laundering / terrorist financing / Combating Financing Terrorism (AML / CFT) and co-operate with the AML / CFT authorities wherever possible and practicable, paying due regard to customer confidentiality and data protection obligations.

2.0. Scope

This Policy is applicable to all services under Ooredoo Mobile Money for all customer types including existing and new mobile wallets, and all types of transactions conducted by OMM's customers, including but not restricted to the following services and any other new services under OMM:

- Mobile Wallets
- Deposits
- Withdrawals
- Remittances
- Airtime top-up
- Wallet to Wallet transfers
- Wallet to Bank account transfers
- Bank account to Wallet transfers
- Wallet to mobile transfers
- Wallet to counter transfers

3.0. Applicability & Exceptions

This Policy applies to:

- All Ooredoo Palestine suspected AML/ CFT operations, and
- All Relevant Banks' AML/ CFT in the course of implementing OMM.
- Mobile money policy will act as a subset of this policy and in case of any conflict, AML policy will supersede

4.0. Definitions

In this Policy, the following words and expressions shall have the meanings hereby assigned to them, unless the context otherwise requires:

The Company	Ooredoo Palestine
AML	Anti-Money Laundering
Money Laundering	Conversion or transfer of property by any person who knows, or should have known, or suspects that such property is the proceeds of crime, for the purpose of concealing or disguising the illicit source of such property, or of assisting any person involved in the commission of the Predicate Offence to escape the legal consequences thereof
CFT	Combating Financing Terrorism
Suspicious Transactions Report (STR)	The format that is agreed with the Relevant Banks to report any suspicious transactions.
Know Your Customer (KYC)	As determined in reference section 6 below, It shall mean comply with all terms related to subscribe to OMM by collecting all necessary information and documents as determined by the Company.
Customer Due Diligence (CDD)	The regular due diligence measures that the Company applies to all customers of OMM.
OMM	Ooredoo Mobile Money
Mobile Wallet	Mobile technology that is used similarly to a real wallet, through which individuals can deposit, withdraw, pay and send money within the country or abroad instantly through their mobile devices
Relevant Banks	All banks and other financial institutions that are partnered with, by the Company to execute OMM.
Enhanced Due Diligence (EDD)	On-going monitoring of OMM transactions of an individual, charity, non-profit organization or other entity that is suspected to be associated with, or involved in, money laundering, terrorist acts, terrorist

	financing or a terrorist organization as referred to in section 7 below
KYE	Know your Employee
Third Parties	Any agents and dealers who provide the services on behalf of the Company
PEP	Politically Exposed Person

5.0. Policy Statements

5.1. Responsibilities of the Company and AML and Compliance function under Revenue Assurance Department:

5.1.1. AML and Compliance function under Revenue Assurance Department, is committed to work with the Relevant Banks to meet their commitments to comply with the AML/ CFT regulations and any relevant international treaties as long as such cooperation will protect the confidentiality and security of its customers' information, and their right to retrieve their information. In this regard, AML and Compliance function will:

- Monitor all OMM transactions in order to identify, detect and prevent any AML/ CFT transactions,
- Collect the Suspicious Activities Reports from the Company and Third Parties with all the relevant information and documents including but not limited to (transferee ID, transfer rates, beneficiaries, transfers destinations and so on).
- Analyse the STRs and forward the credible reports to the Head of the AML and Compliance function for reporting purposes.

5.1.2. The Company and AML and Compliance function will ensure performance of the below principles when customers and employees subscribe to or perform OMM related activities

- **KYC: "Know Your Customer"** during the initiation of all new mobile wallets and on-boarding of any Third Parties
- **KYE: "Know Your Employee"** screening will be performed to assure against the risk of conflicts of interests and susceptibility to Money Laundering Complicity. Coverage will include review of employee's background, job descriptions, and segregation of roles, levels of authority, compliance against codes of conduct and ethics, compliance with laws and regulations, accountability, and other controls.
- **CDD "Customer Due Diligence"** will be conducted on operations and services to reveal possible compliance risks and risks of malpractices, wherever possible using a risk-based approach.

- **EDD "Enhanced Due Diligence**" will be conducted to identify the higher risk**.**

5.1.3. **Transaction Monitoring**: The AML and Compliance function shall continuously monitor all OMM transactions by its customers in order to identify, detect and prevent any AML/ CFT risks.

5.1.4. **Reporting:**
The Head of AML and Compliance function, after obtaining approval from CFO, will raise Suspicious Transactions Report (STR) to relevant banks' Compliance Department along with all the necessary information for further investigations

- The AML and Compliance function at the Relevant Banks will report to the Head of Ooredoo Palestine AML and Compliance function of any AML/CFT activities related to OMM.
- The Head of the AML and Compliance function shall respond to any AML/ CFT questions or requests coming from the Relevant Banks in relation to OMM.
- The AML and Compliance function shall report all STR's to CFO, that have been raised to the regulator (If any). Further, a summary of STR's shall be raised to the Board of Directors via Audit & Risk Management Committee on Quarterly basis, except for material risks / amount of STR, shall be raised to the Board of Directors via Audit & Risk Management Committee as soon as possible.

5.1.5. **Training:** The AML and Compliance function will identify categories of the Company employees and Third Parties needed to undergo AML and Compliance trainings and refresher sessions. The function shall also develop a knowledgebase and conduct examinations to ensure the effectiveness of the conducted trainings.

5.1.6. **PEP "Politically Exposed Persons"**: Appropriate steps will be taken to identify PEPs and their associated risk, including obtaining approval from the CEO and the business's counterpart to initiate new accounts for them.

5.1.7. **Risk Assessment:** The AML and Compliance function under Revenue Assurance Department shall adopt a risk based approach in running its OMM operations, which includes categorizing its customers and their behaviors, and assessing the risk of products and services, systems and controls. This requires a review of new initiatives with taking into consideration risk assessment and change management in order to mitigate any potential financial regulatory risks.

Independent Audit, surprise visits, process/product reviews, and health checks shall take place to assess the overall business compliance, integrity and effectiveness.

In the course of operations, The AML unit/function shall review their internal systems and access rights / business operations periodically and implement any required enhancements.

5.1.8. Appropriate AML System shall be used and integrated with other systems to perform controls defined in the Scope of Works, referred to in Work Instructions in section 6 below.

5.1.9. The Head of AML and Compliance function has the overall responsibility for the establishment and maintenance of effective AML/ CFT and to the control system and act as a focal point for all activities relating to AML/ CFT within the business. The Head shall have a high level of authority, independence, and unrestricted access to resources and information sufficient to enable him to carry out his responsibilities

5.1.10. The AML and Compliance function under Revenue Assurance Department has the Primary responsibility for compliance with the Policy, legislation and regulation, and implementing effective proportionate risk-based on information provided AML/CFT systems and controls.

5.1.11. The AML and Compliance function and shall store all relevant documents and related information in a secure location as per the Company Archiving Policy. Including but not limited to (Compliance Report, Health Check Report, Suspicious Report, KYC - Customer, Employer, Business Partner and Vendor, Business and Service - Agreement and Amendments)

If the function wishes to legally discard any document, which is no longer required, the documents will be completely destroyed prior to disposal.

5.2. Role of Company Employees and Third Parties

Company employees (especially Sales and Call-center) and Third Parties, as the first defense line, shall report any AML/CFT suspicious activities to the AML and Compliance function.

The Company, upon request, shall promptly provide the following to the AML and Compliance function under Revenue Assurance:

1. Access to system applications, data and system databases (mostly read-only access).
2. Internal process documents.
3. Contracts and agreements with vendors/suppliers/partners.
4. Marketing papers, Business rules and any change management process documents

The AML and Compliance function shall maintain the confidentiality of such data entrusted upon them.

The Business shall obtain a formal clearance from AML and Compliance function and prior to the launch of any financial products.

All employees shall report any suspicious behaviour that could lead to, or be a result of AML/CFT activities. The AML function provides assurance that anyone raising a genuine concern will not be questioned nor will they suffer any form of detriment as a result. As long as the employee is acting in good faith. The employee shall communicate such information to the head of AML and Compliance Function

5.3. External Assistance:

The AML and Compliance function under Revenue Assurance Department unit reserves the right to appoint / consult independent body or bodies, whenever the need arises, within the purview of company's policies and the State laws.

5.4. Deviations from this Policy will only be considered in exceptional circumstances. The business shall consult and seek approval from the relevant stakeholders such as; the head of Legal and AML functions and where considered appropriate, request a waiver (permanent) or dispensation (temporary) to the Policy. Requests must clearly set out the aspect(s) of the Policy that cannot be complied with, the reasons for this and for dispensation requests, the actions and timescales that will be taken to bring the business area into full compliance.

5.5. Breaches of this Policy shall be reported to the Head of AML and Compliance as soon as they occur, with remedial action agreed between relevant stakeholders and the Head of AML and Compliance, such incidents shall be documented and tracked.

6.0. Policy Amendment and exception

6.1. This Policy supersedes all previous policies, circulars, memos, instructions on the subject.

6.2. Any changes to the provisions of this Policy shall be reviewed and recommended by the CFO to CEO and in turn to the Audit and Risk Committee and the Board of Directors for final approval.

7.0. Relevant Documentation

- Anti-Money Laundering and terrorism financing Decree Law No. (20) of 2015
- And Its Amendments Issued By The Decree Law No. (13) of 2016
- Decree No. (14) of 2015 Concerning the enforcement of Security Council Resolutions