OOREDOO TUNISIE'S ANTI-MONEY LAUNDERING POLICY

1.0. Purpose

The Purpose from this Policy is to :

- **Guide Financial Institutions:** Assist banks and other financial institutions providing Mobile Money Services (MMS) in complying with Central Bank regulations and statutory requirements on Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT).
- **Establish Effective Controls:** Implement feasible AML controls for early identification of potential money laundering and terrorist financing activities.
- **Proactive Risk Management:** Ensure robust Management Systems and Processes to proactively identify and address gaps that could lead to financial crime.
- **Maintain High Standards:** Uphold the highest standards of AML/CFT compliance within the Company, while cooperating with authorities and respecting customer confidentiality.

2.0. Scope

This Policy is :

- Applicable to all Mobile Money Services (MMS) offered by Ooredoo Tunisia, including all customer types (existing and new mobile wallets) and all transaction types (e.g., deposits, withdrawals, remittances, wallet-to-wallet transfers, etc.).
- Covers all existing and future MMS services offered by Ooredoo Tunisia, including any new services introduced under Mobile Money.

The Policy applies regardless of whether Ooredoo Tunisia directly provides MMS or acts as a Distributor for an independent MMS Provider or a Joint-Venture (JV). In case of a JV, Ooredoo Tunisia will strive to ensure the JV endorses principles similar to those outlined in this Policy.

3.0. Applicability & Exceptions:

This policy:

- Applies to all Ooredoo Tunisie operations suspected of AML/CFT activity.

- Covers AML/CFT compliance of all Relevant Banks involved in the implementation of Mobile Money services.
- The overarching AML policy takes precedence over any conflicting provisions within the Mobile Money policy.

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 Tunisia.

AML - Anti-Money Laundering.

Money Laundering –

- Any intentional act aiming at disguising the illicit source of property or revenue resulting directly or indirectly from a crime or tort punishable by imprisonment for three years or more as well as any offense punishable under the Tunisian regulation.
- Any intentional act aiming of placing, depositing, concealing, camouflaging, integrating or conserving the product coming directly or indirectly from the above offenses.

CFT - Combating Financing Terrorism.

OMM – Ooredoo Mobile Money

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.

MM - 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, by 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 money laundering, terrorist acts, or terrorist financing.

KYE – Know Your Employee.

Third Parties- Any agents and partners 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 Finance Directorate:

AML and Compliance function is committed to work with 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 customer information, and their right to retrieve their information. In this regard:

5.1.1. AML/CFT Compliance Function Responsibilities are as follows:

- Monitor all MM transactions 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 (sender's ID, transfer amounts, beneficiaries' names and nationalities, transfers destinations and other relevant information).
- Analyze the STRs and forward to the Head of the AML and Compliance function for reporting purposes.

5.1.2. Company-wide AML/CFT Principles:

The Company and AML and Compliance function will ensure performance of the below principles when customers and employees subscribe to or perform MM 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 has a reporting obligation divided as follows:

- **STR Reporting to Banks:** The Head of AML and Compliance, after obtaining approval from CXO, will raise Suspicious Transactions Reports (STRs) to the relevant banks' Compliance Departments along with all the necessary information for further investigations.
- **Bank Reporting to Ooredoo:** The AML/CFT Compliance function at the Relevant Banks will report to the Head of Ooredoo Tunisie AML and Compliance function of any AML/CFT activities related in particular to OMM.
- **Bank Inquiries:** 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.
- **Internal Reporting:** The AML and Compliance function shall report all STRs to the Chief Finance Officer (CFO), that have been raised to the regulator (If any). Further, a summary of STRs shall be raised to the Board of Directors via the Audit & Risk Committee on a quarterly basis. For material risks or significant STR amounts, the Board of Directors will be informed via the Audit & Risk Committee as soon as possible.

5.1.5 Training

- The AML and Compliance function will identify categories of the Company employees and Third Parties requiring AML and Compliance trainings and refresher sessions.
- The function will develop a knowledgebase and conduct examinations to ensure the effectiveness of the conducted trainings.

5.1.6. Politically Exposed Persons

Take appropriate steps to identify PEPs and their associated risk, including obtaining approval from the Head of the AML function and the business counterpart to initiate new accounts for them.

5.1.7. Risk Assessment:

- **Risk-Based Approach:** The AML/CFT Compliance function will adopt a risk-based approach to managing OMM operations, including customer risk profiling, product/service risk assessment, and system/control risk evaluation.
- **New Initiative Review:** All new initiatives will undergo a thorough risk assessment and change management process to identify and mitigate potential financial regulatory risks.
- **Internal Controls:** The AML/CFT unit will periodically review internal systems, access rights, and business operations to identify and implement necessary enhancements.

- **Independent Audits:** Regular independent audits, surprise visits, process/product reviews, and health checks will be conducted to assess overall business compliance, integrity, and effectiveness.

5.1.8 AML System and Integration

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. Head of AML/CFT Compliance Responsibilities

- **Overall Responsibility:** The Head of AML/CFT Compliance is responsible for establishing and maintaining an effective AML/CFT framework and monitoring system within the business.
- **Focal Point:** Acts as the central point of contact for all AML/CFT-related activities within the organization.
- **Authority and Resources:** Possesses high-level authority, unrestricted access to resources, and sufficient information to effectively fulfill their responsibilities.

5.1.10 Compliance responsibility:

compliance with the Policy, legislation and regulation, and implementing effective proportionate risk-based on information provided AMI-ICFT systems and controls.

5.1.11. Restoring relevant documentation:

AML function shall store all relevant documents and related information in a secure location for a duration of not less than 10 years as per the Tunisian regulation.

5.1.12. Document Management and Storage

- **Document Custodian:** The AML/CFT Compliance function is responsible for the safekeeping and storage of all relevant AML/CFT documents.
- **Document Access:** The function will provide copies of relevant documents to authorized parties upon request.
- **Automated Database:** The function will implement an automated database for efficient document storage, retrieval, and auditing.

5.2. Role of Company Employees and Third Parties:

Roles of Company Employees and Third Parties are as follows:

- report any AMI-ICFT suspicious activities to the AML and Compliance function.
- promptly provide the following to the AML and Compliance function:

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.

- maintain the confidentiality of such data entrusted upon them
- consider the decision of the Pricing Committee before the launch of any new financial products
- employees shall report any suspicious behavior that could lead to or be a result of AML/CFT activities.

5.3. External Assistance: The AML/CFT Compliance function may engage independent bodies or consultants as needed, within the framework of company policies and applicable laws.

5.4. Policy Deviations: Deviations from this policy are permitted only in exceptional circumstances. Approval from relevant stakeholders (e.g., Head of Legal, Head of AML) is required. Requests for waivers (permanent) or dispensations (temporary) must be justified and include a plan to achieve full compliance.

5.5. Breach Reporting and Remediation: Any breaches of this policy must be reported immediately to the Head of AML/CFT Compliance. Remedial actions will be agreed upon with relevant stakeholders, and all incidents will be documented and tracked.

6.0. Amendments to Policy:

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. References:

- Organic law No, 2015-26 dated on 7th August 2015 relating to the support of the fight against terrorism and the repression of money laundering.
- Organic Law No. 2019-9 of January 23, 2019, amending and supplementing Organic Law No. 2015-26 of August 7, 2015, relating to the fight against terrorism and the repression of money laundering.
- Decision No. 2024-01 of June 27, 2024, issued by the Tunisian Financial Analysis Commission, setting out guiding principles for the reporting of suspicious transactions and operations.