Anti-Money Laundering Policy and Procedures

Compliance and Monitoring Procedures

Version: 2.1
Date: 26-04-2026

Approved by:

Sabah K. Al-Ghunaim
Chairman

شـركة شبـكة الخـدمات الآلـيـة
Automated Services Network Co.

Contents

Introduction:

Automated Services Network Company, eNet is committed to maintaining the highest standards of integrity, transparency, and regulatory compliance in all aspects of its operations. As part of this commitment, The Company has developed this Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) Policy to detect, prevent, and deter illicit activities, including money laundering and terrorist financing. This policy outlines the principles, guidelines, and procedures that govern The Company's efforts to combat financial crime and comply with applicable laws and regulations.

1- Policy Statement

Automated Services Network Company, eNet is dedicated to upholding the integrity of the financial system and protecting its customers, shareholders, and stakeholders from the risks associated with financial crime. The Company recognizes its responsibility to implement effective controls and procedures to mitigate the risk of money laundering and terrorist financing. The company is committed to:

- Compliance with the state of Kuwait Laws, rules and regulations.
- Implementing robust customer due diligence (CDD) measures to verify the identity of customers, assess their risk profile, and understand the nature of their transactions.
- Monitoring transactions and activities to detect and investigate suspicious behavior indicative of potential money laundering or terrorist financing.
- Reporting suspicious activities to the appropriate authorities in accordance with applicable laws and regulations.
- Providing ongoing training and awareness initiatives to employees to enhance their understanding of AML/CFT risks and compliance requirements.
- Regularly reviewing and updating this policy to reflect changes in regulations, the best practices in industry, and emerging risks.

The company is committed to promptly addressing any irregularities that may arise, as we prioritize transparency in all our operations. To uphold this commitment, we have implemented the following policy statements:

"To abide by the rules laid down by the Laws related to the Anti-Money Laundering & Combating Finance of Terrorism of the State of Kuwait, the Central Bank of Kuwait (CBK) AML Regulations and Directives, the FATF and other international organizations guidance relating to AML/CFT, and to assist all the competent authorities in combating Money Laundering and Financing of Terrorism."

The company is committed to the provisions of Circular No. 2/105/9554/2026 regarding Resolution No. 176 of 2025, issued on Dec 09, 2025, concerning the Executive Regulations for implementing the Security Council resolutions issued under Chapter VII of the United Nations Charter related to the fight against terrorism and the financing of the proliferation of weapons of mass destruction.

In Addition to Circulars No. 582/2025, 592/2025, 593/2025, 602/2025

- Circular No. (2/2025/582/رك /رص /أ رت /رت /أ رب /رب), issued on 8 May 2025 by the Central Bank of Kuwait to all electronic money service providers, regarding the **Guidance on the Concept of Beneficial Ownership**.

- Circular No. (2/2025/592/رب/ رب أ/ رص/ رت/ رت أ/ رك), issued on 31 July 2025 by the Central Bank of Kuwait to all electronic money service providers regarding the **Guidance on Combating Proliferation Financing**.
- Circular No. (2/2025/593/رب/ رب أ/ رص/ رت/ رت أ/ رك), issued on 21 August 2025 by the Central Bank of Kuwait to all electronic money service providers, regarding the **Guidance on Proliferation Financing Typologies**.
- Circular No. (2/2025/602/رب/ رب أ/ رص/ رت/ رت أ/ رك), issued on 20 October 2025 by the Central Bank of Kuwait to all electronic money service providers, regarding **Risk Indicators of Proliferation Financing**

The company is committed to the resolution concerning:

- Immediate and prompt compliance with the decisions issued by the sanction committees of the Security Council, as well as decisions aimed at preventing and disrupting terrorism or its financing.
- Providing the Central Bank of Kuwait with all available data and information through the email addresses we have.

Mechanism for Implementing Decision No. (176) of 2025 Regarding Security Council Resolutions, Requiring Financial Institutions to Implement Security Council Decisions Issued Under Chapter VII:

- Verify customers against international sanctions lists (UN Sanctions Lists) as

Consolidated United Nations Security Council Sanctions List | United Nations Security Council Subsidiary Organs, United Nations Security Council Consolidated List | Security Council, Advanced screening search - OpenSanctions, Sanctions List Search and other local and relevant international databases

- Immediately freeze assets without prior notice upon a match.
- Notify relevant authorities such as the Financial Intelligence Unit and the Central Bank.
- Maintain accurate records of the actions taken for ten years as stipulated in the Ministry of Commerce regulations.
- Regularly update databases to ensure ongoing compliance.

2- Definitions:

Term	Description
AML	Anti-Money Laundering
CFT	Combating Financing of Terrorism
AML Law	Law 106 of 2013
CBK Regulations	CBK Circular No. (2/BS, IBS, FS, IFS, ES, PS/524/2023) and any relevant instructions.
CDD	The process of verifying the identity of customers, assessing their risk profile, and understanding the nature of their transactions to mitigate the risk of money laundering and terrorist financing. CDD measures include customer identification, verification, and ongoing monitoring.
CO/MLRO	Compliance Officer/Money Laundering Reporting Officer
Company	Automated Services Network Company, eNet
EDD	Enhanced Due Diligence – it is the method of collecting additional evidence and answers about a customer and or a transaction during an investigation procedure.

KYC	Know Your Customer - it is the process that the financial services providers and other regulated entities must perform to identify their customers (existing or prospecting), collect and record relevant information, static and professional/business related data.
ML	The process of disguising the proceeds of criminal activity to make them appear legitimate. This may involve placement, layering, and integration of illicit funds into the legitimate financial system.
Money Laundering Risk	It refers to the risk of been engaged directly or indirectly with money laundering, terrorist financing, or proliferation.
CBK	Central Bank of Kuwait
Risk-based approach	It is a regulatory framework that requires institutions to assess the risk associated with their customers, products, services, transactions and business activities.
TF	Terrorist Financing - it is the act of Providing funds or financial support to individuals or groups engaged in terrorist activities or organizations designated as terrorists by relevant authorities. Terrorist financing may involve the use of legitimate financial channels to fund terrorist acts or support terrorist organizations.
Office of Foreign Assets Control (OFAC)	It is an agency of the United States Department of the Treasury under the auspices of the Under Secretary of the Treasury for Anti-Terrorism and Financial Intelligence. OFAC administers and enforces economic, and trade sanctions based on U.S foreign policy and national security goals against targeted foreign states, organizations, and individuals. The Specially Designated National List is a publication of OFAC which lists individuals and organizations with whom United States citizens and permanent residents are prohibited from doing business.
Suspicious Activity	Any transaction or activity that is unusual, inconsistent with the customer's known profile or business activities, or lacks a clear legitimate purpose. Suspicious activities may indicate potential money laundering or terrorist financing and require further investigation and reporting.
Suspicious Transaction Report (STR)	A suspicious Transaction Report (STR) is a report regarding suspicious or potentially suspicious financial activity, filed with the Central Bank of Kuwait and the Financial Intelligence Unit (if differs).
Politically Exposed Persons (PEPs)	"Politically Exposed Persons" mean individual who are, or have been, entrusted with prominent public functions in Kuwait or foreign country, such as Heads of State or government, senior politicians, senior management, judicial or military officials, senior executives of state-owned corporations or important political party officials. Business relationships with family members or close associates of PEPs involve reputational risks like PEPs themselves. The definition is not intended to cover middle ranking or more junior officials in the foregoing categories. Kuwaiti PEPs would include all ministers, all MPs and all MPs, and all Ministry Officials with the rank of Undersecretary or above.

Tipping Off	"Tipping off" refers to the unauthorized disclosure of information to a suspected individual or entity, alerting them that they are under investigation for potential money laundering or terrorist financing activities.

3- Scope:

(a) Purpose:

The purpose of this Policy is to describe the fundamental principles that all members of the company must fully comply with, regarding Anti-Money Laundering (AML) legal and regulatory framework and the legal and regulatory framework of Combating the Financing of Terrorism (CFT).

(b) Scope

The Policy applies to The Company's employees and associates, as described in the applicable law(s), regulations, or directives of the State of Kuwait, relating to the prevention of the use of the financial system for the purpose of money laundering and financing of terrorism.

(c) Responsibility

The functional responsibility of this Policy lies with the Compliance Officer

4- Risk-Based Assessment

This study is conducted to assess the company's exposure to money laundering and terrorist financing risks, and includes:

- **Customer Classification**: Categorizing clients based on risk level, including activity, country, and type of service.
- **Product and Service Analysis**: Evaluating the potential vulnerability of products and services to misuse.
- **High-Risk Distribution Channels**: Identifying high-risk channels such as electronic services or agents.
- **Geographic Risk Assessment**: Focusing on high-risk countries according to the FATF risk ratings.
- **Periodic Updates**: Regularly updating the study based on regulatory or operational changes.

5- Public policy:

It is the Company's policy to prohibit and prevent money laundering and any activity that facilitates money laundering, terrorist financing or criminal activity. The Company generally defines money laundering as engaging in acts intended to disguise the true origin of money raised from criminal act so that the illicit income appears to derive from or constitute legitimate assets.

The Fundamental Principles Include:

- Compliance with the Kuwaiti Anti-Money Laundering Law No. 106 of 2013 and its amendments.
- Adherence to the recommendations of the Financial Action Task Force (FATF).
- Rejection of dealings with entities or individuals listed in international sanctions lists.
- Implementing a risk-based approach to identify and monitor suspicious activities.
- Promoting a compliance culture within the company through continuous training.
- Cooperating with regulatory authorities and disclosing any suspicious transactions.
- The policy is approved by the Board of Directors and reviewed annually or as needed.

In general, money laundering takes place in three stages:

1- **Placement**: In the placement stage, individuals or entities involved in illegal activities, such as drug trafficking or corruption, seek to introduce their illicitly obtained funds into the financial system. This can involve purchasing orders or using other means to place the illicit funds into the legitimate economy.

2- **Layering**: Once the illicit funds are placed into the financial system, the next stage is layering. During this stage, the launderers conduct a series of complex financial transactions to obscure the origin and ownership of the funds. This can include transferring funds between multiple accounts, converting currencies, making investments, or engaging in other transactions designed to create a complex web of financial activity that makes it difficult to trace the funds back to their illegal source.

3- **Integration:** The final stage of money laundering is integration. In this stage, the laundered funds are reintroduced into the economy in a way that makes them appear legitimate. This can involve investing the funds in legitimate businesses, purchasing real estate or other assets, or using the funds to finance further illegal activities. The ultimate goal of integration is to make the illicit funds indistinguishable from funds obtained through legal means, allowing the launderers to enjoy the proceeds of their criminal activities without attracting suspicion.

Terrorism financing may not include finance of criminal behavior, but rather an attempt to conceal the source or intended use of funds, which may subsequently be used for criminal purposes.

Because the Company facilitates purchases and collection of funds, there is a very small but real risk of criminal activity using the Company's money consolidation tools.

6- Work Procedures, Systems, and Internal Controls

These outline how the policy is practically applied within the company and include:

- **Know Your Customer (KYC) System**: Collecting and verifying accurate data before opening accounts.
- **Automated Transaction Monitoring**: Using customer behavior analysis software to detect unusual activities.
- **Suspicious Transaction Reporting (STR)**: Reporting to the Financial Intelligence Unit when suspicious transactions are identified.
- **Segregation of Duties**: Ensuring no conflict of interest between departments.

- **Internal Audits**: Reviewing compliance with procedures and identifying any gaps.
- **Employee Training**: Educating staff on identifying indicators of money laundering and terrorist financing.

7- Appointment and Roles/Responsibilities of the Compliance Officer

(a) Appointment:

The Company has appointed a Compliance Officer who shall be responsible for overseeing the implementation and enforcement of the Anti-Money Laundering (AML) & Combating Financing of Terrorism (CFT) policy and procedures outlined herein.

(b) Qualifications:

The Compliance Officer shall possess a comprehensive understanding of AML/CFT laws, regulations, and best practices, along with relevant experience in the financial services industry. Additionally, the Compliance Officer shall demonstrate strong analytical skills, effective communication abilities, and the capacity to work independently and collaboratively with various stakeholders.

(c) Roles and Responsibilities:

The Compliance Officer shall have the following duties and responsibilities:

- Develop, implement, and periodically review the Company's AML/CFT policies, procedures, and controls to ensure compliance with applicable laws and regulations.
- Conduct risk assessments to identify and evaluate potential money laundering and terrorist financing risks inherent in the Company's operations.
- Monitor transactions and conduct due diligence on customers, counterparties, and other relevant parties to detect and mitigate suspicious activities.
- Provide ongoing training and support to employees to ensure awareness of AML obligations and enhance their ability to identify and report suspicious activities.
- Coordinate with internal departments and external authorities, including regulators and law enforcement agencies, on AML-related matters.
- Conduct periodic reviews and audits to assess the effectiveness of AML controls and recommend enhancements as necessary.
- Maintain thorough documentation of AML activities, including suspicious activity reports (SARs) and related investigations, in accordance with regulatory requirements.
- Ensure the confidentiality and protection of sensitive information related to AML activities to prevent unauthorized disclosure or tipping off potential criminals.

In accordance with the requirements of the law, the compliance officer duty is to act as the Anti-Money Laundering Program Compliance Officer, with full responsibility for the Company's Anti-Money Laundering (AML) Program which includes the following:

1- Effectively implement the company's anti-money laundering program, including monitoring the compliance of the company's officials and employees with their obligations under the program.

2- Updating the anti-money laundering program annually.

3- That the employees of the company properly trained to implement the program.

4- Reporting and sharing anti-money laundering information with the Kuwaiti Financial Intelligence Unit and the concerned authorities about any suspicious operations related to money laundering or terrorist financing. Respond to any request from the concerned authorities and search our records to determine whether we maintain or have maintained any account or participated in any transaction with any individual, entity or organization inquired about.

(d) Compliance Governance and Reporting Line

The Compliance functions are managed by the Compliance Officer, who reports directly to the Board of Directors and the Compliance and Governance Committee.

The Compliance Department operates independently and overseas:

- KYC and onboarding
- Transaction monitoring
- Screening Sanctions
- Periodic reviews
- Regulatory reporting

8- Weapons of mass destruction

This policy aims to prevent the use of eNet services in facilitating or financing activities related to the production, transfer, or spread of weapons of mass destruction (WMD), including nuclear, chemical, biological weapons, or any dual-use materials that could be used for such programs.
The company is committed to adhering to the following:

- United Nations Security Council (UNSC) resolutions related to WMD proliferation.
- The U.S. Office of Foreign Assets Control (OFAC) regulations.
- Financial Action Task Force (FATF) standards on anti-money laundering (AML) and combating the financing of terrorism and WMD proliferation.
- Any relevant local or international regulations.

The company does not provide its services to any shell companies or companies operating under the guise of other entities.

9- Check the Sanctioned Lists

Before approving any request potentially involving money laundering, we will check to ensure that the applicant does not appear on the list of the sanctioned lists and is not from or involved in transactions with persons or entities from embargoed countries and regions listed on the Anti-Money Laundering Office website, and by searching on search engine sites or social media, there is no similarity against him, and work will be done with the competent authorities to provide a search mechanism at the earliest opportunity. If it is found that the applicant, or a person dealing with or for him, may be on the list of the sanctioned list or engage in transactions with a person or entity located in a country or region subject to the embargo, the application will be rejected.

10- Identifying and Verifying the Applicant

We have created, documented, and maintained a written application system. A minimum amount of applicant identification information will be collected from each applicant, and we give notice to applicants that we will request identification information and compare applicant identification information with the lists of sanctioned as set out above in #4.

(a) Required applicant information.

Before the application is approved, the following information will be collected for all applicants: name; Address (which would be the individual's residential or commercial street address); Identification number, which will be the civil ID number or one or more of the following: resident ID number, and country of issue of any other government-issued document proving nationality or residency and bearing a photo or other similar guarantees (for non-Kuwaiti persons). As well as the contact number, which is the landline or mobile phone number, and we will not approve any request if the applicant applies for it and does not meet these conditions.

(b) Applicants who refuse to provide information

If a prospective or current applicant refuses to provide the information described above upon request, or appears to have provided intentionally misleading information, their application will be rejected and in either case, the AML Compliance Officer will be notified.

(c) Verify information

Based on risk, and to an extent reasonable and practicable, it is ensured that we have a reasonable belief that we know the true identity of our applicants by using risk-based procedures to verify and document the accuracy of information we obtain for our applicants.

To verify the identity of the applicant, we analyze any logical inconsistencies in the information we obtain. We verify the applicant's identity through documentary evidence, non-documentary evidence, or both. We use the documents to verify the identity of the applicant when the appropriate documents are available. Considering the increasing incidence of identity fraud, we may supplement the use of documentary evidence by using the non-documentary means described below whenever possible. We may also use such non-documentary means, after using the documentary evidence, if we are still not sure whether we know the identity of the applicant. When analyzing verification information, we look at whether there is a logical consistency between the identifying information provided, such as the applicant's name, street address, postal code, telephone number (if provided), date of birth, and Civil ID number.

Appropriate documents to verify the identity of applicants include, but are not limited to, the following:

- An unexpired government-issued ID proving citizenship and residency and holding a photograph or similar guarantees, and small projects license.
- For companies, a license from the Ministry of Commerce is requested and the authorized person signs and the address of the company is verified.
- We understand that we are not required to take steps to determine whether a document provided to us by an applicant for identification verification has been properly issued and

that we may rely on government-issued identification to verify an applicant's identity. However, if we observe that the document shows an obvious form of fraud, we must take this factor into account in determining whether we can form a reasonable belief that we know the true identity of the applicant.

(d) Record keeping

We will keep records of all identifying information and verification information obtained for ten years after receiving any application.

(e) Notice to applicants

Notice will be placed to applicants that the Company will request information from them to verify their identities, as required by law. Notice to applicants regarding the policy will be given either orally or in the form of a clearly posted notice such as:

"To assist the government in combating terrorist financing and money laundering activities, the law requires us to obtain, verify, and record information that identifies each person who applies for financial services from eNet. We will ask for your name, address, and other information that will allow us to identify you. We may also ask to see Your driver's license, passport or other identification documents."

11- Customer Due Diligence Procedure

Customer Due Diligence (CDD), Enhanced Due Diligence (EDD) Policy and Know your customer KYC Policy

Objective:

This section outlines the due diligence requirements that eNet, under the Central Bank of Kuwait (CBK), implement to comply with Anti-Money Laundering and Counter-Financing of Terrorism (AML/CFT) regulations, including Law No. 106 of 2013, CBK circulars, and FATF recommendations.

(a) Know Your Customer (KYC) – Foundation of Due Diligence

Definition:

KYC is the process of identifying and verifying a customer's identity, understanding the nature of their activities, and assessing the risk they pose before providing financial services.

KYC Objectives:

- Verify Customer Identity
- Prevent money laundering and terrorism financing.
- Establish a risk-based customer profile.
- Ensure compliance with regulatory obligations.
- Enable monitoring of customer behavior and transactions
- Protect the company from the risk of reputation.

(b) Basic Customer Due Diligence (CDD)

1. Collection of Identity Information

- **For Legal Entities:**

Field	Description
Registered legal name	As per commercial license
Commercial registration number	Verified with relevant authority
Business activity	Nature of operations
Registered address	Corporate address
Authorized signatories	Names and valid IDs
Ultimate Beneficial Owner (UBO)	Required for ownership ≥25%
Screening against sanctions lists for Merchants, Employees and Third-Party Vendors before onboarding	OFAC, UN, EU, SC, local lists, CBK Circulars all accounts listed on eNet system with other adverse media check portals

2. Identity Verification

- Match provided documents with national databases or trusted third parties.

3. Understanding Purpose and Intended Nature of Relationship

- What service is required?
- Intended use? (Personal use, business-related)
- Anticipated transaction volume and frequency.

4. Customer Risk Profiling

Each customer is assigned a risk rating based on:

- Geographic location (e.g., high-risk jurisdictions)
- Nature of business
- Source of funds and wealth
- Transaction patterns
- Legal structure (individual vs. shell company)

Risk Tiers:

- Low Risk
- Medium Risk
- High Risk

(c) Enhanced Due Diligence (EDD)

Applied in cases such as:

- Politically Exposed Persons (PEPs)
- Customers from FATF high-risk jurisdictions
- Those whose Kuwaiti citizenship has been revoked and against whom an order has been issued to amend their residence.
- Complex or non-transparent business structures
- High-value or unusual transactions.
- Businesses classified as high-risk according to the Central Bank of Kuwait circular

EDD Measures Include:

Requirement	Details
Proof of source of wealth	Contracts, Proof of ownership document
Screening against sanctions lists	OFAC, UN, EU, SC, local lists, CBK Circulars all accounts listed on eNet system with other adverse media check portals
Senior management approval	Before onboarding high-risk customers
Enhanced monitoring	Daily transaction reviews, anomaly tracking

Enhanced Due Diligence (EDD) Mechanism and Requirements for High-Risk Clients and Politically Exposed Persons (PEPs):

PEPs are individuals who hold prominent public positions and must be handled with caution through the following:

- Conducting Extensive Business Activity Checks: Examining the business activities of traders in detail.
- Obtaining Senior Management Approval: Securing approval from senior management before opening the account.
- Continuous Transaction Monitoring: Ongoing monitoring of transactions for any suspicious activities.
- Periodic Updates of Personal and Financial Data: Regularly updating personal and financial information to ensure accuracy.

(d) Ongoing Monitoring

- Use of **automated transaction monitoring systems** to detect anomalies.
- Periodic review of customer files (at least annually for high-risk customers) or whenever changes requested to company structure.
- Monitoring for:
  - Transactions inconsistent with expected behavior
- Revalidation of KYC information when:
  - Customer risk profile changes
  - Red flags are triggered

(e) Customer Data Update Periods Based on Risk Level

1. High-Risk Customers

- Refresh Frequency: Every 12 months (maximum)
- Required Actions:
  - Full identity
  - Review of transaction history and activity patterns
  - Updated sanctions and PEP (Politically Exposed Person) screening
  - Adverse media checks (negative news screening)

2. Medium-Risk Customers

- Refresh Frequency: Every 2 Years
- Required Actions:
  - Basic identity verification update
  - Transaction pattern review

- screening sanctions

3. Low-Risk Customers

- Refresh Frequency: Every 3 years
- Required Actions:
    - Confirmation of basic contact details
    - Automated transaction monitoring (no manual review required unless flagged)
    - Passive screening via AML/CFT systems

Triggers for Out-of-Cycle Reviews

1. Significant change in customer activity
2. Changes in ownership structure (for corporate clients)
3. Unusual or suspicious transactions
4. Negative media exposure
5. Change in the risk rating of the customer's country
6. Alerts from automated monitoring systems

(f) Reporting & Compliance

Obligation	Requirement
Suspicious Transaction Reports (STR)	Must be submitted to Kuwait Financial Intelligence Unit (KWFIU) using goAML portal within 48 hours of suspicious activity detection and freezing merchant payments. **1. Suspicious Transaction Report (STR)** • The STR is used to report any transaction that is suspected to be related to money laundering or terrorist financing. Steps: 1. From the main menu, select "Report → New → STR. 2. Enter the customer's or entity's information (full name, civil ID or commercial registration number, and address). 3. Specify the type of suspicious activity (e.g., fund transfers, electronic transactions, unusual account usage, etc.). 4. Provide a detailed description of the reason for the report and the nature of the suspicion. 5. Describe the circumstances surrounding the discovery of suspicion and any internal actions taken (such as internal escalation or transaction review). 6. Upload all supporting documents related to the suspicious transaction, such as: o Details of the suspicious transaction o Civil ID / Passport copy o Bank account details o Commercial registration and business license o Account opening form o Know Your Customer (KYC) form o Any other relevant supporting documents

Obligation	Requirement
	7. Include financial transactions and account details related to the individual or entity used in the suspected money movement. 8. Click Submit to send the report to the Kuwait Financial Intelligence Unit (KWFIU) through the goAML system. **2. Follow-up and Correspondence** • The status of the report can be tracked within the system as: Submitted / Under Review / Closed. • If the Financial Intelligence Unit requires additional information or documentation, a notification will be sent through the system or via the registered email. • The company must respond to such requests within the specified timeframe set by the FIU.
Record retention	Minimum 10 years after the termination of relationship or execution of the last transaction
Internal audit & review	Semi-annual AML/CFT compliance assessments
Staff training	Mandatory annual training on CDD, EDD, red flags, and regulatory obligations

12- Foreign correspondent accounts and fictitious foreign banks

It is our policy that the Company will not provide any financial services to companies outside Kuwait or when we have reasonable cause to believe that an institution is involved in any way in suspicious financial transactions.

13- Monitoring operations for suspicious activity

(a) Signs of danger

These signs of potential money laundering or terrorist financing include, but are not limited to:

- The applicant shows unusual concern about the company's compliance with government reporting requirements and anti-money laundering policies, is reluctant or refuses to disclose any information regarding personal financial affairs or provides unusual or suspicious identification or documents.
- Upon request, the applicant either declines to disclose or fails to provide valid documentation—such as invoices—to substantiate substantial financial transactions.
- The applicant (or anyone publicly associated with the applicant) has a questionable background or is the subject of news reports indicating possible criminal, civil, or regulatory violations.
- The applicant shows a lack of interest in the costs of services.
- The applicant finds it difficult to describe the nature of his/her work.

- The applicant makes unjustified or surprise payments involving monetary instruments are in an amount slightly below the reporting or registration thresholds Example: 3,350 KWD payment).
- The applicant requests that the transaction be processed to avoid the company's normal documentation requirements.
- The applicant has inflows of funds that far exceed the agreed upon volume.

(b) Respond to signs of danger and suspicious activity

When a responsible Company employee detects any sign of danger, he or she will conduct further investigation under the direction of the Anti-Money Laundering Compliance Officer. This may include collecting additional information internally or from external sources or contacting government agencies. The company is obliged to report suspicious transactions that are made or attempted to be made through it or through its clients.

(c) Responsibility for anti-money laundering records

The AML Compliance Officer and his/her designers are responsible for ensuring that AML records are properly maintained.

(d) Monitoring for Spikes in Authorization Attempts:

Objective: Detect unusual activity that may indicate fraud, bot attacks, or system errors.
Process:
Thresholds are set based on historical transaction volumes for each merchant.
Real-time monitoring systems track authorization attempts.
If the volume of attempts exceeds the threshold (e.g., 3 times or more the normal pattern within a specific time frame), alerts are automatically triggered.
Alert Handling:
Alerts are sent to the Monitoring Team for immediate review.
Automated email is sent to the merchant requesting the invoice/documents related to the identified transactions.

(e) Alert Management and Escalation Workflow

Steps:
Alert Generated (real-time via monitoring platform)
Preliminary Review by Monitoring team.
Investigation using transaction logs, merchant history checks.
Decision Point:
No issue found: Alert closed with documentation.
Suspicious activity confirmed:
Transactions may be blocked.
Merchant account may be suspended.
Further information requested from the merchant.
Follow-Up Actions: May include reporting to regulators, updating monitoring rules, or initiating a merchant audit.

(f) Stakeholders Involved

Stakeholder Role:

- Risk Monitoring Team: Monitors alert and perform first-level investigations.
- Risk and Compliance Team: Conducts detailed reviews and ensures regulatory compliance.
- Merchant Services/Operations: Communicates with merchants, gathers additional info, and manages account actions.
- IT Security: Investigates technical anomalies and ensures platform integrity.
- Legal & Regulatory (as needed): Supports high-risk cases and regulatory escalations.
- Senior Management: Engaged in high-severity or reputational risk cases.

14- Required records.

As part of our anti-money laundering program, the Company or its clients shall create and maintain other relevant documentation relating to and verifying the applicant's identity. It also maintains these records and accompanying documents for at least ten years. The Anti-Money Laundering Compliance Officer shall conduct an annual or whenever necessary inspection of related files and records, provided that a list of the files that have been inspected and the actions that must be taken in any of them are recorded in the event of any observations.

15- Training programs:

- The company provides continuous internal training sessions for its employees every year or when necessary and the training is carried out by the Compliance Officer and/or Information Technology Department or through suitable training services for a third party.
- Our operations are reviewed to see if certain officers or employees require additional specialized training.
- Our written procedures are updated to reflect any such changes.

16- Testing the anti-money laundering program:

- Annual testing of our Anti-Money Laundering Program is conducted either by a qualified independent third party or internally by a qualified corporate officer. Annual testing includes a review of our compliance with our anti-money laundering program.
- The auditor issued a report on his findings upon completion of his audit to the Board of Directors.
- We approach each of the resulting recommendations meticulously and professionally.

17- Monitoring employee behavior and accounts

All employee financial transactions are subject to the same Anti-Money Laundering (AML) procedures as applicant and customer accounts, under the supervision of the Company's AML Compliance Officer.

Transactions conducted by the AML Compliance Officer are independently reviewed by a qualified officer within the Company to ensure objectivity and compliance with internal controls.

Employee information and accounts are monitored through advanced screening tools, including United Nations Security Council Consolidated List | Security Council, Consolidated United Nations Security Council Sanctions List | United Nations Security Council Subsidiary Organs, and other local and relevant international databases, to detect any potential risks or irregularities.

18- Vendor Due Diligence

The Company shall apply a risk-based approach when conducting due diligence on all Vendors, in compliance with the instructions of Central Bank of Kuwait related to AML/CFT, outsourcing, and electronic payment service providers.

1. Regulatory Compliance and Licensing

- Verify that the Vendor is duly licensed and regulated by the competent authority.
- Ensure the Vendor complies with all relevant laws and regulations in Kuwait.
- For regulated activities, confirm no regulatory breaches or penalties issued by Central Bank of Kuwait or other authorities.

2. Identification and Verification

- Obtain and verify:
  - Commercial License
  - Memorandum & Articles of Association
  - Authorized signatories
- Validate the legal existence and operational status of the Vendor.

3. Beneficial Ownership (UBO) Requirements

- Identify and verify the Ultimate Beneficial Owner(s).
- Obtain ownership structure charts.
- Ensure transparency of ownership in line with CBK guidelines.

4. Sanctions and Name Screening

Conduct screening of the Vendor, its UBOs, shareholders, and management against:

- United Nations (UN) Sanctions Lists
- European Union (EU) Sanctions Lists
- OFAC Lists
- Local lists issued by:
  - Ministry of Foreign Affairs
  - Ministry of Commerce and Industry
  - Central Bank of Kuwait

5. Risk-Based Classification

- Classify Vendors as Low / Medium / High Risk based on:
  - Nature of service (e.g., payment processing, outsourcing critical functions)
  - Geographic exposure (high-risk jurisdictions)
  - Access to customer funds or sensitive data
  - Regulatory supervision level

6. Information Security and Data Protection

- Evaluate Vendor's cybersecurity framework.
- Ensure compliance with data protection and confidentiality requirements.

- Confirm secure handling of customer data and payment information.

7. Contractual Requirements

All Vendor agreements must include:

- AML/CFT compliance obligations
- Adherence to CBK regulations
- Termination rights in case of non-compliance

8. Approval and Escalation

- Compliance Department approval is mandatory.
- High-risk Vendors require Senior Management or Board approval

9. Ongoing Monitoring and Review

- Periodic review of Vendor risk profile.
- Continuous sanctions screening.
- Monitoring performance, compliance, and any regulatory changes.

19- Confidential reporting of non-compliance with anti-money laundering

Company employees shall report any violations of the Company's Anti-Money Laundering Compliance Program to the Anti-Money Laundering Compliance Officer, unless the violations relate to the compliance officer, in which case the employee must report it to the appropriate member of the Board of Directors. These reports are confidential, and the employee will not suffer any retaliation for submitting them.

20- Additional areas of risk

The Company reviews all areas of its business to identify potential money laundering risks that may not have been covered in the procedures described above and is constantly improving its anti-money laundering program.

21- The approval of the Board of Directors

The Board has approved this Anti-Money Laundering Program as reasonably designed to achieve and monitor the Company's ongoing compliance with Central Bank of Kuwait (CBK) regulations, Anti-Money Laundering and Counter-Financing of Terrorism (AML/CFT) regulations, including Law No. 106 of 2013, CBK circulars, and FATF recommendations.

22- Policy Review

Finally, we need to update our Anti-Money Laundering Policy and Procedures - Compliance and Monitoring Procedures periodically annually.