AML and KYC POLICY

FINANCING OF TERRORISM, ANTI-MONEY LAUNDERING, KNOW YOUR CUSTOMER

POLICIES AND PROCEDURES

1. FOREWORD

This Policy provides guidelines and procedures ("**Policy**") applicable to DIFX Africa PTY Limited (hereinafter referred to as "**DIFX**" or "**Company**") also known as **DoshFX** (brand name used in African region) that are intended to serve as a useful reference guide to the Company regarding measures for combatting of money laundering, prevention of financing of terrorism or criminal activities, or of any such related activity. The increasing incidents of financial crimes have highlighted the serious threat to the integrity of financial systems, and the further requirement to take measures to prevent and combat such crimes. It can be briefly described that money laundering is the process by which proceeds from criminal activity are disguised to conceal their illegal and illicit origin.

Money laundering incidents have commonly been amalgamated with drug trafficking where the drug proceeds are laundered through the financial system.

Criminals are now taking advantage of the globalization of the world economy by transferring funds very quickly across international borders than ever before with the help of rapid developments in the financial and banking sector, information technology plays a vital core role to communicate and allows money to move anywhere in the world with speed and ease. This makes the task of combating money laundering more crucial than ever.

Therefore, the Company has developed and implemented this Policy using a risk-based approach to address the risk of money laundering specific to the Company's services, customers, and business partners to comply with the applicable law and to combat money laundering and terrorist financing, and other financial crimes. This Policy includes international guidelines and recommendations that were necessary to combat money laundering and the financing of terrorism. The Company makes every attempt to inform and train our employees to understand the money laundering and combating terrorist financing so that employees can further assist in detecting, preventing, and eradicating these crimes.

2. INTRODUCTIONS

2.1. GENERAL PRINCIPALS

2.1.1. The goal of criminal operations is to generate a profit for the individuals or group that carries out the activity. Money laundering is the processing of these criminal proceeds disguised as legal. This process is of critical importance as it enables the criminal to enjoy these earnings without jeopardizing themselves or their other activities.

2.1.2. Institutions involved in financial activities and related activities are required by law to identify, monitor, investigate and report transactions of a suspicious nature to the Financial Intelligence Centre in respective jurisdictions. All these institutions must verify a customer's identity (due diligence) by obtaining the required documents for further understanding of the kind of transactions in which the customer is likely to engage, to make sure that funds do not involve money laundering.

2.1.3. DoshFX shall implement several anti-money laundering and combating the financing of terrorism measures as required under applicable international standards and recommendations. DoshFX has policies designed and

procedures implemented to identify any suspicious activities and ensure that any transaction routed through is not used by criminals or terrorists.

2.1.4. With more emphasis to have a transparent business environment in both services to customers and compliance, it is considered sufficient to meet the requirements of the regulations, as in force within the Republic of South Africa and to ensure compliance with FATF Recommendations, UN and other international regulatory bodies (where applicable).

2.1.5. This Policy will be reviewed annually and updated (when required) and will be approved by the Chief Executive Officer & Head of Legal and Managing Director.

2.2. **ENFORCEMENT**

2.2.1. Any Company employee found to have violated this Policy will receive a warning letter. Multiple (two or more) violations of this Policy will result in the termination of employment of the violating employee.

2.2.2. Employees will go through the AML compliance training arranged by the Company (see clause 3 of this Policy) and be aware of the consequences of their failure to comply with the Policy, including reporting potential fraudulent/suspicious activities that may lead to the employee's voluntary or involuntary involvement into criminal activities.

2.2.3. Any third-party partner found to have violated this Policy will be subject to contract termination as well as any other remedial measures available under applicable law.

2.3. **DEFINITIONS**

2.3.1. "**HEAD OF AN INTERNATIONAL ORGANIZATION (HIO)"** means individuals who are or were previously entrusted with a prominent function by an international organization such as members of senior management or individuals entrusted with equivalent functions (i.e. directors, deputy directors, members of the board or equivalent functions) and such individual's family members and close associates.

2.3.2. **"ULTIMATE BENEFICIAL OWNER** OR **THE UBO"** means the 'Natural Person' who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a juridical person. A natural person who owns 5% or above of the juridical person is treated as a UBO.

2.3.3. **"SOURCE OF FUNDS"** means how the money, involved in the transaction, was originally derived, or earned. Examples of sources of funds are salary, wages, inheritance, gratuity, end-of-service benefits, bank loan, income from businesses, sale of property, sale of land, sale of investments, etc. For verification of the Source of funds, documents include but are not limited to salary slips, labor contracts, court orders, bank statements, etc.

2.3.4. "**PURPOSE OF TRANSACTION"** means an explanation about why a customer is conducting a transaction or the reason for which the funds will be used. For verification of the purpose of the transaction, documents may include any documentation proving the purpose for which the money will be used.

2.3.5. **"DUE DILIGENCE" -** Refers to the measures taken to mitigate risk before entering into an agreement or carrying out a financial transaction with another party.

2.3.6. **"KYC"** – Know Your Customer is the process of verifying the identity of the customer. The objective of KYC guidelines is to prevent banks from being used, by criminal elements for money laundering activities

3. EMPLOYEE TRAINING

3.1 The Company will ensure that its employees are familiar with the key compliance requirements applicable to the Company's activities. Further, the Company will develop an ongoing employee compliance training program that will explain:

- The Policy's requirements, and principles and procedures related to compliance
- The requirements of compliance under the applicable law
- The Company's record-keeping and reporting obligations
- Guidance in identifying suspicious activity or transactions conducted
- Guidance in identifying money laundering operations
- The procedure to be followed once the risks provided in this policy are identified (including how, when, and to whom to escalate red flags for analysis)
- What the employees' roles are in the Company's compliance efforts and how do perform them
- The disciplinary consequences (including civil and criminal penalties) for non-compliance; and
- The key business risks and the results of the risk analyses enable the employees to take them into account in the course of their work routine.

3.2 As a part of the training, each employee will participate in quarterly AML training (video-based). Each shall undertake an assessment and receive handout materials highlighting the means and mechanics to detect and prevent money laundering. The materials if required will be updated by the Company on an annual basis or within the timeline as may be decided by the Company.

4. MONEY LAUNDERING AND FINANCING TERRORISM

4.1. DEFINITIONS

- **MONEY LAUNDERING** refers to any transaction aimed at concealing and/or changing the identity of illegally obtained money so that it appears to have originated from legitimate sources, where in fact it has not".

- **FINANCING OF TERRORISM** refers to any act that provides financing or financial support to individual, entities, or state which is involved in terrorist activities.'

4.2. MONEY LAUNDERING RELATED ACTS AND REGULATIONS

- Organized criminal activity & racketeering
- Human Trafficking & migrant smuggling
- Dealing in Narcotics & Psychotropic substances
- Counterfeiting currency & piracy of products
- Insider trading & market manipulation
- Sexual exploitation, including children
- Kidnapping, piracy & terrorism
- Offences committed in violation of environmental laws
- Illicit dealing in firearms & ammunition

- Bribery, embezzlement, damage to public property
- Corruption, fraud, breach of trust & related offences

4.3. STAGES OF MONEY LAUNDERING

- **PLACEMENT**

  Introduction or placement of illegal proceeds into the financial system is termed as 'Placement'. Often, this is accomplished by placing the funds into circulation through financial institutions.

- **LAYERING**

  The separation of illicit proceeds from their source by layering of financial transactions intended to conceal the origin of the proceeds is called 'Layering'. This second stage involves converting the proceeds of the crime into another form and creating complex layers of financial transactions to disguise the audit trail, source, and ownership of funds.

- **INTEGRATION**

  This stage entails using laundered proceeds in seemingly normal transactions to create the perception of legitimacy. The launderer, for instance, might choose to invest the funds in real estate, financial ventures or luxury assets.

  By the integration stage, it is difficult to distinguish between legal and illegal wealth. This stage provides a launderer the opportunity to increase his wealth with the proceeds of crime.

  Integration is generally difficult to spot unless there are great disparities between a person's or company's legitimate sources of legitimate employment, business or investment ventures and a person's wealth or a company's income or assets.

4.4. TERRORIST FINANCING

Terrorist Financing is a facility of providing financial support to terrorist groups or individual terrorists. Terrorist Financing may include both legitimate funds and proceeds of criminal conduct. The most common legitimate funds sources are charitable donations and legitimate sources include foreign government sponsors, business ownership and personal employment.

4.5. DIFFERENCE BETWEEN MONEY LAUNDERING AND TERRORIST FINANCING

The main difference between money laundering and financing of terrorism is the origin of funds, in the case of financing of terrorism funds can be from legitimate sources as well. The motivation differs between traditional money launderers and terrorist financiers. The actual methods used to fund terrorist operations can be the same as, or similar to, methods used by other criminals to launder funds. Funding for terrorist attacks does not always require large sums of money and the associated transactions may not be complex.

4.6. RISK OF MONEY LAUNDERING AND THE FINANCING OF TERRORISM FOR DOSHFX

Money Laundering and Financing of Terrorism carries a number of risks which includes but not limited to:

- A breach of legislation and regulation for AML/CFT may show a weak compliance control of the Company and may cause civil and criminal penalties including jail term against the members of the Company.

- Reputational risk of the Company.

- Liquidity risk in the Company capital cashflow in case compliance/legal risks and reputation risks are realised due to the involvement in money laundering, Company may suffer from getting funding from markets to realise the bearing costs.

- Solvency risk in the worst case the solvency of the company may be threatened.

- Operating licenses may be withdrawn or denied.

4.7. **CONTROLS**

In order to prevent an adverse impact above, the Company employs automatic and manual control systems, that allow the Company to analyse transactions over various periods of time across all its customers in order to determine whether structuring or other illegal or suspicious activity has occurred or is occurring.

4.7.1 MANUAL CONTROLS

Fraud Monitoring Department

The Company has incorporated a fraud monitoring department that is responsible for detecting suspicious transactions and is responsible for detecting and preventing fraud.

4.7.2 EMPLOYEES ROLE

Each employee is responsible for detecting and reporting suspicious transactions. If a transaction seems suspicious, it probably is. If employees recognize any of the red flags discussed above during a transaction, they should ask themselves the following questions:

- Is the amount of the transaction unusually large for the typical customer?
- Does the customer make the same or similar transactions more frequently than normal?
- Does the type of transaction seem unusual for the customer?

An employee must report any detected suspicious transaction (along with supporting documents) to the Company via email ID.

4.7.3 CHANGE AND DEVELOPMENT

The existing internal controls have been formulated and implemented in accordance with the business structure of the Company. The internal controls are based on the risks arising out of the Company's business activity and will be developed and improved along with the Company's business growth.

5. **COMPLIANCE PROGRAMME**

5.1. DoshFX firmly believes in conducting business procedures in compliance with applicable regulatory requirements and provides a secure and legitimate environment and service to customers.

5.2. A strong, properly designed, documented compliance program ensures that the Company works within the regulatory ambit where any non-compliance issues are timely identified, reported, and actioned upon. Minimum requirements for a comprehensive compliance program include, but not limited to:

- Compliance Strategy
- Compliance Framework
- Risk Management and Compliance Program
- ML/FT Risk Assessment
- AML/CFT Policies and Procedures

- Independent Compliance Officer
- Sanctions Program
- Know Your Customer Policies
- Training
- Transaction Monitoring
- Record Retention
- Reporting

5.3 Compliance Roles and Responsibilities

- Establish and maintain appropriate AML/CFT policies, procedures, processes and controls.
- Ensure day-to-day compliance of the business against internal AML/CFT policies and procedures.
- Receive suspicious transaction alerts from employees and analyse them to take appropriate decisions to report all suspicious cases to the Financial Intelligence Centre using the Go AML system.
- On-going monitoring of transactions to identify high-risk, unusual, and suspicious customers/transactions.
- Submit STR to the FIU in a timely manner.
- Develop and execute AML/CFT training programs considering all relevant risks of ML/FT and financing illicit organizations including the ways/means for addressing them.
- Arrange to retain all necessary supporting documents for transactions, KYC, monitoring, suspicious transaction reporting and AML training for the minimum period for record retention.

6. REPORTING REQUIREMENTS

The Company recognizes that reporting of any wrongdoing is among the government's main and primary weapons in the battle against money laundering and other financial crimes. The Company will report all necessary details of its activity in accordance with the requirements prescribed in the applicable laws.

6.1. SUSPICIOUS TRANSACTION REPORT

A Suspicious Transaction Report ("**STR**") is a report on the detected suspicious activity of the Company's customers. STRs are among the government's main weapons in the battle against money laundering and other money services crimes. Such reports are also a key component of an effective compliance program in this Policy.

Suspicious transactions must be reported if the Company knows, suspects, or has a reason to suspect that the transaction or linked transactions:

- Involve funds derived from illegal activity or intended or conducted in order to hide or disguise funds or assets derived from illegal activity.
- Designed to evade the reporting requirements, whether through structuring or other means.
- Serves no business or apparent lawful purpose and the Company knows of no reasonable explanation for the transaction after examining all available facts.
- Involves any other use of the Company or its services to facilitate criminal activity.

6.2. **INTERNAL REPORTING**

All employees must report any activity that they see in the course of their duties and that they think may be suspicious to the compliance department. The Company shall provide all necessary training and guidance to ensure that the employees are aware of:

- Their obligations in this area
- Possible offences and penalties for not disclosing or reporting any suspicious activity
- Any internal disciplinary sanctions that may apply for not reporting
- Procedures to be followed
- Description of all the red flag indicators
- Documentation to be used to make reports; and
- Where to receive further advice and guidance.

7. **MONEY LAUNDERING /FINANCING TERRORISM RISK ASSESSMENT**

- Money laundering/Financing terrorism ("**ML/FT**") risk assessment provides reasonable assurance that essential ML/FT risk that may impact well-being of an organization have been identified and appropriate mitigating controls have been implemented.
- Compliance Department needs to be conducted annual risk assessments for ML/FT. Risk Assessment report along with findings, possible solution, and implementations.

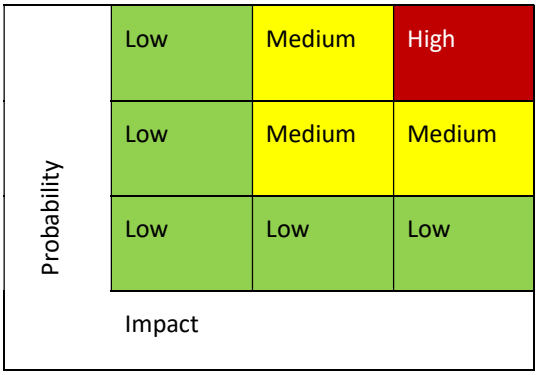
7.1. **ML/FT RISK ASSESSMENT METHODOLOGY**

Risk assessment shall be conducted to review all the processes which are prone to ML/FT risk. It must be ensured that appropriate controls are in place and effectively implemented. ML/TF risks associated with the following parameters must be evaluated at a minimum:

- Customer Risk
- Counterparty Risk
- Product / Services Risk
- Jurisdiction Risk
- Delivery Channel or Interface Risk

7.2. **RISK RATING MATRIX**

The following Risk Rating Matrix will be applied while assessing regulatory requirement risk and its impact:



8. **<u>KNOW YOUR CUSTOMER (KYC)</u>**

8.1. **RISK BASED APPROACH**

DoshFX has a continued risk-based approach to KYC process to aggregate a precise measure for the AML risk of the customer. The approach has been implemented to identify and mitigate risks of abuse of the Company's services by potential and existing customers or any third party. Customer availing the services of the Company requires Customer Due Diligence ("**CDD**") and High-Risk Customer requires Enhanced Due Diligence ("**EDD**") to be performed. The following are the risk factors that have been considered to mitigate the risks:

8.1.1. Geography

The approach is evaluated on the following risk indicators which includes the country of the customer, country of the customer's employment or place of business. Based on several factors provided by international bodies such as FATF, UN, OFAC, etc, DoshFX will risk rate countries as Low or high risk.

8.1.2 Customer

Customers shall be identified as high-risk customer if falling under the categories of High Net-Worth / Private / PEPs / HIO. High risk customers shall require EDD in accordance with this Policy.

8.1.3 Business

The unemployed customers are considered as high risk and there are the following other businesses which are considered as high risk:

- Banks, Financial Institutions, and similar companies
- Insurance companies,
- Companies operating in Real Estate
- New or used car dealers
- Sea / Air / Land Transportation companies
- Export / Import
- Oil and Gas
- Mining and metal trading
- Free Zone / Off-shore Entities

- Jewellery and Precious Metals Dealers
- Telemarketing / Online Service Providers
- Hotels and Resorts
- Supermarkets, restaurants and laundromats

8.2. **PROHIBITED DEALINGS**

DoshFX upon the KYC assessment with the risk-based approach will not establish relationship and perform transaction for the entities which are involved in the below-listed trading/business activities:

- NGOs/Societies/Not for Profit Making Organization
- Shell Company
- Shell Bank
- Alcohol Trading (if not licensed)
- Arms and Weapons dealerships
- Online betting and casinos
- Hawaladars
- Trusts
- Individuals / Entities in the Sanctions List or Internal Blacklist

Please note that the above-mentioned list is not exhaustive and will be updated from time to time by the Company.

9. **DUE DILIGENCE FOR ONBOARDING AND TRANSACTION**

DoshFX carry out KYC process to identify who the real customer is and ensure legitimacy of the funds involved in their transactions. KYC process has been divided into 3 categories,

- Customer Identification (CID)
- Customer Due Diligence (CDD)
- Enhanced Due Diligence (EDD)

9.1. **NATURAL PERSONS (INDIVIDUAL)**

9.1.1. Customer Identification

The customer identification process involves verification of the original identification documents for customer and recording the listed below information in system:

- Customer full legal name
- Mobile Number
- Nationality
- Date of Birth
- ID Type
- ID Number

9.1.2. Customer Due Diligence

CDD process is to be done by the Company every time the customer's pattern or a particular transaction looks suspicious, and the Company has to confirm the legal nature of the transaction. The level of CDD performed in such cases depends on the particular circumstances raising suspicions. CDD process involves obtaining additional information about customer in addition to completing CID process. No transaction will be processed unless the customer successfully completed CDD to the Company's full satisfaction.

A. CUSTOMER ONBOARDING PROCESS

To use the Company's services, a customer must provide consent on the Company to retain and process the customer's personal information and share it with third parties on as needed basis to provide the services to the customer. The Company is responsible for safeguarding the customer's data from unauthorized disclosure.

A customer must register to use Company's services. The customer will have to enter the following personal information in addition to the details recorded in the system for CDD process.

- Email, if available
- Country of birth
- ID expiry details
- Profession
- Expected annual income
- Source of funds
- Purpose of transactions
- Method of payments

B. INTERMEDIARY CHECK

Accounts open in fake names or nicknames will be blocked, and the customer will be requested to correct the account information by providing it within three days from the request of the Company. Generally, the system doesn't allow the registration of accounts with incomplete information. However, if such an account has been registered (for instance, using two letters as a street name), it will be checked and closed if the fake information provision is confirmed.

C. PEP DECLARATION

The customer will have to state whether the customer is a politically exposed person ("**PEP**") or not, in other words, whether such customer:

- Is or has been entrusted with prominent public functions in the Republic of South Africa or any other foreign country such as head of states or governments, senior politician, senior government official, judicial or military official, senior executive manager of state-owned corporations, and senior official of political parties and a person who is, or has previously been, entrusted with the management of an international organisation or any prominent function within such an organisation

- Is an immediate family member or a known close associate of a person referred to in the immediately preceding paragraph

- Individuals having joint ownership rights in a legal person or arrangement or any other close business relationship with the PEP; and

- Individuals having individual ownership rights in a legal person or arrangement established in favor of the PEP.

- Information will be automatically uploaded into the Company's records and stored there until the customer requests to perform a transaction.

- If a customer claims to be a PEP, the customer will be requested to pass both the stages of the EDD process provided in this Policy. Additionally, senior management approval will be sought before entering into a business relationship with the PEP. Senior management will be notified if an existing customer becomes a PEP.

D. SANCTION LISTS SCREENING

All customers' details are screened against the UNSC Consolidated Lists ("**Sanctions lists**") in the course of the customer's onboarding process.

E. TRANSACTIONAL THRESHOLDS

Depending on the amount of the transaction and the type of service requested, the customer will be required to provide additional information as may be requested by the Company, unless otherwise decided by the Company in case of suspicious activity and/or transaction.

The Company uses CDD on account creation as described in accordance with this Policy. Such a risk-based approach allows the Company to prevent an abuse of its services by potential criminals, including money launderers, without creating an excessive burden for small customers using the service randomly for explicitly transparent transactions.

9.1.3. Enhanced Due Diligence

EDD requires (in addition to what has been mentioned under CID & CDD) DoshFX to verify and confirm sources of funds and purpose of transaction, based on following points:

- Evidence of sources of funds must be collected.
- Complete information of the purpose of the transaction must be gathered.
- Appropriate evidence must be collected for the verification of the purpose of the transaction (in case there is any doubt or suspicion about the information provided).

9.2. **LEGAL PERSONS (ENTITY)**

9.2.1. Enhanced Due Diligence

Legal Entities require EDD at the time of onboarding and processing their transaction. The EDD process for the customer at the time of onboarding includes but not limited to:

Verification of the identity, its beneficial owners and authorized representative and other onboarding requirements by collecting the following valid documents and information:

- Copies of Commercial License/Trade License (or equivalent)
- Copies of Certificate of incorporation
- Copies of Certificate of Incumbency
- Copies of Memorandum of Association (MoA)
- Copies of Share Certificate/Share Register (where details of shareholders are not available in MoA)
- Copies of Documents providing details of Ultimate Beneficial Owners
- KYC Questionnaire
- Trading agreement
- Purpose and nature of the intended business relationship. (BOR)
- Copies of identification document of Owner(s) (passports/ID cards)
- Authorization letter must be taken for representative of the legal entity who carry out transaction on its behalf
- Copies of documents providing details of relationship with the company and powers of authorized signatories who have authorization to carry out transactions on behalf of the Company along with their identification documents. Such representative must be UAE residents.
- Compliance approval is required prior onboarding legal entity.
- If Legal entity or any of its UBOs/Authorized signatory is found to be FPEP, then onboarding should be completed only after obtaining approval from Managing Director/Chief Executive Officer of DoshFX.
- Residential status & address (whether incorporated/operating from, etc)
- Phone numbers
- FPEP/PEP status
- Appropriate evidence must be collected for the verification and confirmation the sources of funds, purpose of the transaction and commercial / economical reason for each transaction.
- The receipt must be signed by the representative of the legal entity who carries out the transaction on its behalf and must be retained in the records.

9.3. **THIRD PARTY TRANSACTIONS**

It is prohibited to accept third party transactions except in certain cases and with conditions as per following scenarios:

9.3.1. Natural Person on behalf of another natural person

- The representative must produce a duly executed Power of Attorney (POA) from the beneficial owner of the funds to carry out such transactions. In the absence of POA the beneficial owner of funds should issue a letter giving authority to the representative to carry out transaction on his/her behalf.

  The letter:
  - ✓ Validity should not exceed 1 year from the date of issue.
  - ✓ Must provide clear details about the type of transaction which is allowed.
  - ✓ Provide identification details of both parties i.e. beneficial owner and representative.
  - ✓ Contains details of beneficiary (Name, nationality, country of fund transfer, beneficiary bank details)

- ✓ Must be signed by both parties.

- The signature of the beneficial owner of funds in the letter of authority must be verified against that in the passport or ID cards.
- KYC process to be completed for the beneficial owner of the funds as well as representative
- All measures practically possible must be taken and extreme care must be applied to confirm that the transaction is genuine. In case of doubts/confusion regarding the documents submitted or information provided by the representative.

9.3.2. Natural Person on behalf of legal person

Natural person performing transaction on behalf of legal entity falls under the scope of EDD.

- It must be ensured that supporting documents, such as invoices, are in the name of legal entity
- EDD must be performed prior to onboarding such customer and beneficial Owner of the Funds.
- At least one shareholder / partner must be common to both entities
- Must not accept any transactions from a natural person, who is acting in personal capacity, on behalf of any foreign entity

9.4. **FREQUENCY OF DUE DILIGENCE**

9.4.1. Natural Person (Individual)

It must be ensured that the customer profile shall be reviewed and updated either annually or upon the expiry of the identification documents whichever comes first. The original ID must be verified, and copy must be held in the records during the review of customer profile.

9.4.2. Legal Persons (Entity)

DoshFX must be ensured to repeat EDD and customer profile, including the supporting evidence of entity registration and UBOs / authorized signatory identification documents must be updated annually at a minimum. It must be ensured that copies of valid documents must be always present in records.

EDD must also be performed whenever there is a change in the recorded profile of the customer e.g. change in ownership, business activities, etc.

10. **SANCTIONS COMPLIANCE**

10.1. **COUNTRY RISK ASSESSMENT**

10.1.1. Data from several sources such as FATF, corruption precipitation index, internal policy etc. will be used to assign rating to each country to arrive at accumulated rating for each country.

10.1.2. Compliance department will perform country risk assessment on annual basis.

10.1.3. Results of risk assessment will be presented to **Compliance Committee** and decision will be taken on the way forward

11. **TRANSACTION REVIEW**

- Sanction compliance is one of the key requirements from not only local regulators but also international regulatory authorities. DoshFX has a strict policy to ensure compliance with applicable Sanctions requirements.

- DoshFX will make sure that not to deal with individual / entities which are listed in the sanctions list.

- All customer onboarding / transactions must be screened against local / international / FPEP / internal blacklist.

- For corporate transaction compliance department will manually screen correspondent bank name against sanctions list for each transaction.

12. **TRANSACTION MONITORING**

- Transaction monitoring is ensuring that DoshFX does not become a tool to launder money or finance terrorism and only genuine transactions are processed through DoshFX.

- Transaction monitoring involves scrutinizing the transaction to ensure that transactions are consistent with customer, business, risk profile, sources of funds, annual transaction activity, etc.

- DoshFX has implemented system to monitor and identify suspicious transactions and generate alerts for abnormal/suspicious transactions.

13. **RECORD RETENTION**

- DIF DoshFX responsibility is to retain the records as per regulatory requirements under the applicable laws. Records include electronic communication and documentation as well as physical, hard copy communication and documentation. According to DoshFX record retention policy all the records are keeping for 10 years period.

- The electronic copies of the documents will be stored on the Company's server at a secure location with limited access granted to certain employees on an as needed basis. Paper documents will be kept in safe boxes by the responsible employees.