



**IGI Funds
Limited**

**Know Your
Customer/Customer Due
Diligence Policy**

Table of Contents

- 1 INTRODUCTION**
 - 1.1 Ownership**
 - 1.2 Purpose of Policy**
- 2 MONEY LAUNDERING**
 - 2.1 The Money Laundering Process**
 - 2.2 Individual Employee Duties**
- 3 MONEY LAUNDERING AND FINANCIAL INSTITUTIONS**
 - 3.1 Policies, Procedures and Internal Controls**
- 4 CUSTOMERS / INVESTORS DUE DILIGENCE**
 - 4.1 High Risk Customers / Investors**
 - 4.2 Low Risk Customers / Investors**
- 5 CUSTOMERS / INVESTORS ACCEPTANCE**
 - 5.1 Account Opening**
 - 5.2 Account Information & Documentation**
 - 5.3 Verification**
- 6 REPORTING**
 - 6.1 Suspicious Transaction Report**
 - 6.2 Critical Transaction Report**
 - 6.3 Monitoring for Suspicious Activity**
- 7 RECORD UPDATION**
- 8 RECORD RETENTION**

1 INTRODUCTION

The attempted use of financial institutions to launder money is a significant problem that has resulted in the passage of stricter laws and increased penalties for money laundering including the Anti Money Laundering Act, 2010. This Policy (“Policy”) is designed to establish principles and standards to protect against attempts at laundering money.

This Policy is to be used to create an understanding among employees concerning the risks of laundering money and the penalties for failing to comply with the procedures outlined herein. This Policy establishes the standards to which IGI Funds Limited (“the Company”) should adhere.

1.1 Ownership

This Policy is applicable to the Company and is enforced by the Company’s Head of Operations. Changes to the Policy may be made only with the recommendation of the Head of Operations, Risk Manager and the Compliance Officer and approved by the CEO and BOD.

1.2 Purpose of Policy

This policy contains procedures to ensure that the Company complies with the applicable anti-money laundering laws and regulations and protect against its involvement in money laundering, terrorist financing and illegal trades by:

- Introducing to the employees the stages of money laundering process and to their individual duties;
- Establishing a review process which will be used to identify opportunities that might be used to launder money;
- Defining Guidelines that will promote knowing who our customers / investors are; and
- Providing instructions regarding taking appropriate action once a suspicious activity or a money laundering activity is detected or suspected.

Customers of the Company include Unit Holders of Funds being managed by the Company as well as advisory customers.

2 MONEY LAUNDERING

Money laundering is the involvement of any transaction or series of transactions seeking to conceal or disguise the nature or source of proceeds derived from illegal activities, including drug trafficking, terrorism, organized crime, fraud, and other crimes.

2.1 The Money Laundering Process

Generally, the money laundering process involves three stages:

1. Placement - The way criminal funds enter the system i.e. physically disposing of cash derived from illegal activity. One way to accomplish this is by placing criminal proceeds into financial institutions or non-traditional financial institutions such as currency exchanges.

2. Layering – How the link between the funds and the criminal is concealed i.e. separating the proceeds of criminal activity from their source through the use of layers of financial transactions. These layers are designed to hamper the audit trail, disguise the origin of funds and provide anonymity.

3. Integration - Placing the laundered proceeds back into the economy in such a way that they re-enter the financial system as apparently legitimate funds.

The degree of sophistication and complexity in a money laundering scheme is infinite, limited only by the creative imagination and expertise of the perpetrator. It is possible for a person with criminal intent to make use of a financial institution, such as an insurance company, at any point in the money laundering process.

2.2 Individual Employee Duties

The Company expects that its employees will comply with applicable money laundering laws. It also expects that its employees will conduct themselves in accordance with the code of conduct.

The Company's employees are prohibited from providing advice or other assistance to individuals who attempt either to violate or avoid anti-money laundering laws or this Policy. Such assistance may include, but is not limited to, approving suspicious applications or new group accounts, or the failure to thoroughly analyze the source of client funds, or failing to meet obligations as outlined in this Policy.

The Company's employees whose suspicions are aroused by suspicious activities (which will be more fully described later in this Policy), but who fail or neglect to make further inquiries, may be considered to have knowledge of such activity. The Company's employees who suspect money laundering activities must refer the matter to the Head of Operations.

Failure to adhere to this Policy may subject the Company's employees to disciplinary action up to termination of employment. Violations of anti money laundering laws may also subject the Company and the Company's employees to fines, forfeiture of assets, and other serious punishment, including imprisonment.

3 MONEY LAUNDERING AND FINANCIAL INSTITUTIONS

For money laundering to be successful, the “paper trail” must be eliminated or at least made complex to separate each of the steps. Within the financial system, money launderers may structure transactions, coerce employees to cooperate and not to file proper reports, or establish apparently legitimate “front” entities to launder money. Some “red flags” include, but are not limited to the following:

- Unusual payment methods, such as cash or cash equivalents.
- The transfer of benefits of a product to an apparently unrelated third party.
- A customers / investors who is reluctant to provide identifying information.

We have developed this Policy with the understanding that different money laundering risks arise depending on the types of products sold, services provided and the distribution channel in which it is marketed.

3.1 Policies, Procedures and Internal Controls

Policies, procedures and internal controls must be developed, based on the company’s assessment of the money laundering risk associated with its business, that are reasonably designed to enable the insurance company to comply with the applicable requirements of the Anti Money Laundering Ordinance, 2010 and to prevent the company from being used by money launderers.

4 CUSTOMERS / INVESTORS DUE DILIGENCE

The Company shall carryout Customers / Investors Due Diligence, and shall classify its customers / investors into High Risk Customers / Investors and Low Risk Customers / Investors, based on the following parameters of risk perception:

- the nature of business activity;
- location of customer / investor and his clients;
- mode of payments;
- volume of turnover;
- social and financial status;
- reliability of data / information furnished; and
- behavior of the customer / investor.

4.1 High Risk Customers / Investors

Operation department should conduct enhanced due diligence when:

- a) Dealing with high-risk customers / investors, business relationship or transaction including the following:
 - a. Non-resident customers / investors;
 - b. Non-legal persons or arrangements including non-governmental organizations (NGOs) / not-for-profit organizations (NPOs) and trusts / charities;
 - c. Customers / Investors belonging to countries where CDD / KYC and anti-money laundering regulations are lax;
 - d. Customers / Investors with links to offshore tax havens;
 - e. High net worth customers / investors with no clearly identifiable source of income;
 - f. Customers / Investors dealing in high value items.
- b) There is reason to believe that the customer / investor has been refused by another financial institution.
- c) Dealing with politically exposed persons (including foreigners) or customers / investors holding public or high profile positions. For politically exposed persons or holders of public or high profile positions, enhanced due diligence should include the following:
 - a. Relationship should be established and / or maintained with the approval of senior management including when an existing customer / investor becomes holder of any public office or high profile position.
 - b. Appropriate risk management systems shall be put in place to determine whether a potential customer / investor, existing customer / investor or the beneficial owner, is a politically exposed person, holder of public office or holder of a high profile position. The sources of wealth / funds of such customers / investors should be monitored on regular basis.
- d) Establishing business relationship or transactions with counterparts from or in countries not sufficiently applying Financial Action Task Force (FATF) recommendations.

4.2 Low Risk Customers / Investors

Where there are low risks and information on the identity of the customer / investor and the beneficial owner of a customer / investor is publicly available, or where adequate checks and controls exist, Operation Department may apply simplified or reduced CDD / KYC measures. The following cases may be considered for application of simplified or reduced CDD / KYC:

- a) Financial institutions provided they are subject to requirements to combat money laundering and terrorist financing consistent with the FATF recommendations and are supervised for compliance with those requirements.
- b) Public listed companies that are subject to regulatory disclosure requirements, Government administrative / entities.

5 CUSTOMERS / INVESTORS ACCEPTANCE

The Company shall follow the following guidelines in customers / investors acceptance:

- i. No account is opened in anonymous or fictitious / benami name(s);
- ii. Parameters of risk perception are clearly defined in terms of the nature of business activity, location of customers / investors and his clients, mode of payments, volume of turnover, social and financial status etc. To enable categorization of customers / investors into low, and high risk customers / investors requiring very high level of monitoring, e.g. Politically Exposed Persons (PEPs) may, if considered necessary, be categorized even higher.
- iii. Not to open an account or close an existing account where the Company is unable to apply appropriate customers / investors due diligence measures i.e. IGI Funds is unable to verify the identity and /or obtain documents required as per the risk categorization due to non cooperation of the customers / investors or non reliability of the data/information furnished to the IGI Funds.
- iv. Circumstances, in which a customer / investor is permitted to act on behalf of another person / entity, should be clearly spelt out in conformity with the established law and practice of IGI Fund as there could be occasions when an account is operated by a mandate holder or where an account is opened by an intermediary in fiduciary capacity and
- v. Necessary checks before opening a new account so as to ensure that the identity of the customers / investors does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations etc. For list of prohibited entities use the following URL.
<http://www.un.org/sc/committees/1267/consolist.shtml>

The Company has applied enhanced due diligence measures based on the risk assessment, thereby requiring intensive 'due diligence' for higher risk customers / investors, especially those for whom the sources of funds are not clear.

5.1 Account Opening

True identity of the customers / investors should be established before opening an account. No business transactions should be conducted with customers / investors who fail to provide evidence of their identity.

For individuals, identity can be established by obtaining a copy of their passport, national identity card or any other document, which can substantiate the customers / investors' name, address, date of birth, citizenship, and signature. In case of non-residents, copies of passports must be obtained.

For corporate entities, identity can be established by certificate of incorporation or registration. In case of any doubt, the customers / investors should be asked to provide documentary evidence of its existence and validity. Except for well-known national or multinational organizations, it would be prudent to obtain copies of passports or national identity cards of all authorized signatories of the account.

Physical location of the customers / investors should be stated in the account opening form. PO Box may be used only for correspondence.

For all customers / investors, the Account Officer should determine whether the customers / investors is acting on behalf of another person, and should then take reasonable steps to obtain sufficient identification data (such as copy of CNIC, or other relevant document/information) to verify the identity of the beneficiary.

For customers / investors that are legal persons or for legal arrangements, the Account Officer is required to take reasonable measures to:

- i. Understand the ownership and control structure of the customers / investors
- ii. Determine the natural persons who ultimately own or control the customers / investors. This includes those persons who exercise ultimate effective control over a legal person or arrangement.

Government accounts should not be opened in the personal names of the government official(s). Any such account, which is to be operated by an officer of the Federal / Provincial / Local Government in his / her official capacity, shall be opened only on production of a special resolution / authority from the concerned administrative department duly endorsed by the Ministry of Finance or Finance Department of the concerned Government.

5.2 Account Information & Documentation

1. Individual Account/Sole Proprietorship:

- Name, Father Name, Address, Telephone Number completely filled in.
- Copy of passport or CNIC.
- Sources of Income (In case of retired individual customers / investors, a declaration will be obtained to this effect)
- Business / Employment proof (e.g. business card/employment card/pay slip/NTN/Letter from employer etc.)
- KYC form to be duly filled and signed by customers / investors along with application form.

2. Partnership Account:

- Name of Partnership and Partners, Father Name of partners, Addresses, Telephone Numbers completely filled in.
- Duly filled in completed and signed by the authorized signatory.
- KYC form to be duly filled and signed by customers / investors along with application form.
- Copies of passports or CNICs of all the partners and authorized signatories,
- Certified copy of partnership deed,
- Certified copy of registration certificate where applicable.
- Copy of latest financials of partnership firm.
- Certificate of registration.

3. Limited Company Account:

- Name of Company and its directors, Registered Address, Telephone Numbers completely filled in.
- Copy of passports / CNICs of all the directors.
- Certificate of incorporation.
- Memorandum and articles of association;
- Board Resolution.
- Latest available audited accounts of the company.
- KYC form to be duly filled and signed by customers / investors along with application form.

The company secretary, under his hand and the company's stamp, should certify all the above listed corporate documents.

The memorandum and articles of association should be reviewed by the Account Officer to check that these documents authorize the business, which the company is engaged in and that the persons authorized to act in the board resolution have been duly appointed in terms of the same.

4. Club Society, Association, or Trust Account:

- KYC form to be duly filled and signed by customers / investors along with application form.
- Board / Trustee / Governing body Resolution.
- Copies of passports / CNICs of trustees / authorized signatories,
- Certified list of office bearers / trustees,
- Resolution of the management committee / trustees,
- Copy of the constitution / rules / bye-laws / trust deed.
- Certificate of registration.
- Latest financials of the club / society / association / trust.

5.3 Verification

The Account Officer should verify Customers / Investors' CNIC by utilizing the on-line facility of NADRA. Operations department should verify the information given in the KYC form.

6 REPORTING

Once the Company has notified that there is a risk that the Company has been involved in a money laundering scheme or that there are suspicious that such an activity might occur, the process of reporting the activity will begin.

6.1 Suspicious Transaction Report

The Company shall file with the Financial Monetary Unit Suspicious Transaction Report, not later than seven working days after forming that suspicion, conducted or attempted by, at or through the Company if the Company knows, suspects, or has reason to suspect that the transaction (or a pattern of transactions of which the transaction is a part):

- involves funds derived from illegal activities or is intended or conducted in order to hide or disguise proceeds of crime;
- is designed to evade any requirements of the law; or
- has no apparent lawful purpose after examining the available facts, including the background and possible purpose of the transaction.

6.2 Critical Transaction Report

The Company shall not deal in cash transactions therefore filing Critical Transaction Report is not applicable to the Company. However, if any such instance occurs, CTR will be filed to the Financial Monetary Unit immediately, but not later than seven working days.

6.3 Monitoring for Suspicious Activity

The Company shall monitor its customers / investors' relationships to detect any suspicious activities. Suspicious activities include many ordinary transactions, which may be legitimate, but should be examined.

In the event that any suspicious activity is detected, Suspicious Activity Report shall be filed to the Financial Monetary Unit immediately, but not later than seven working days.

7 RECORD UPDATION

CDD/KYC is not a one-time exercise to be conducted at the time of entering into a formal relationship with the customers / investors / account holder. This is an on-going process and to this end, the Operations department is required to:

- a) Put in place a system to monitor the accounts and transactions on regular basis
- b) Update customers / investors information and records, if any, at reasonable intervals.
- c) Chalk out a plan of imparting suitable training to the staff of Operation department periodically.
- d) Maintain proper records of customers / investors identifications and clearly indicate, in writing, if any exception is made in fulfilling the CDD / KYC measures.

8 RECORD RETENTION

Operation department shall keep records regarding the identification data obtained through the customers / investors due diligence process (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence for at least five years after the business relationship is ended.

In case operation department is not able to satisfactorily complete required CDD/KYC measures, an account should not be opened, business relationship should not be established and business transactions should not be carried out. Instead, reporting of suspicious transactions should be considered. Similarly, relationship with existing customers / investors should be terminated and reporting of suspicious transaction should be considered if CDD/KYC is found unsatisfactory.