Anti-Money Laundering & Combatting the Financing of Terrorism Policy

(Last updated: March 2024)

POLICY STATEMENT

Axiory Global Ltd (the "Company") is committed to providing excellent service to its customers while ensuring compliance with all regulatory requirements. One of the key components of the Company's compliance programme is its Anti-Money Laundering & Combatting the Financing of Terrorism Policy (the "Policy"), which outlines the procedures and processes for identifying and verifying the identity of new customers, conducting customer due diligence checks, and assessing the risk of each customer.

To achieve this goal, the Company has established this Policy that will define the principles and arrangements to be employed by the Company for it to conduct its business with due skill, care and diligence, in order to mitigate the risk of financial crime, including money laundering and terrorist financing, and to protect the integrity of the Company and the wider financial system. By implementing this Policy, the Company aims to build trust with its customers and demonstrate its commitment to ethical business practices.

AXIORY

TABLE OF CONTENTS

I. INTRODUCTION AND PURPOSE

The purpose of this Policy is to summarize the approach and internal practice, measures, procedures, and controls relevant to the prevention of Money Laundering and Terrorist Financing of the Company.

The Company shall ensure the policies and procedures established include systems and controls that:

(a) enable it to identify, assess, monitor and manage money laundering and terrorist financing ("ML-TF") risk; and
(b) are comprehensive and proportionate to the nature, scale and complexity of its activities.

To prevent ML-TF, the Company shall comply with anti-money laundering and counter-terrorism financing ("AML-CFT") laws, verify the identity of customers, and assist government agencies and financial organizations working to combat money laundering.

The Belize AML-CFT legislative framework consists of the following legislations:

- Money Laundering and Terrorism (Prevention) Act 2020, as amended by the Money Laundering and Terrorism (Prevention) (Amendment) Act 2023
- Financial Intelligence Unit Act 2014

Additionally, the Company follows the recommendations of the Financial Action Task Force ("FATF"), which is an independent inter-governmental body that develops and promotes policies to protect the global financial system against ML-TF and the financing of the proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global standards in respect of AML-CFT.

II. SCOPE

This Policy applies to the Company, all of its staff, contractors, vendors, and any other individuals who interact with the Company in the course of their business activities.

III. COMPLIANCE WITH THIS POLICY

All of the Company's staff, contractors, vendors, and any other individuals who interact with the Company in the course of their business activities, must have knowledge of, and comply with, this Policy. Failure to comply with this Policy may result in disciplinary action as appropriate.

The Company recognizes that failure to comply with this Policy could lead to legal or regulatory actions against the Company, its directors, shareholders, staff, and agents. Therefore, the Company emphasizes the importance of strict adherence to this Policy in order to prevent fraudulent activities and maintain the integrity of its operations.

IV. RISK ASSESSMENT

The Company has a duty to identify, assess and understand its ML-TF risks, and establish policies, controls and procedures to mitigate and manage effectively the risks identified in any risk assessment taken by the Company. In this respect, the Company should:

(a) understand its ML-TF risks; and
(b) have in place effective policies, procedures and controls to:
    (i) identify
    (ii) assess
    (iii) understand
    (iv) mitigate
    (v) manage, and
    (vi) review and monitor those risks in a way that is consistent with the AML-CFT requirements and this Policy.

The Company adopts a risk-based approach to managing ML-TF risks and determining:

(a) appropriate levels of customer due diligence measures, including whether to apply enhanced due diligence measures;
(b) mitigation measures commensurate with the risks posed by the Company's customers, business relationships, countries or geographic areas, services, delivery channels, products and transactions;
(c) measures for detecting and reporting suspicious activity; and
(d) whether and how to launch new products, services or technologies.

The Company shall manage its ML-TF risks in an analytical and considered way and establish and maintain policies, procedures and controls that are specific, appropriate and proportionate to the risks its senior management identifies. Risk assessments shall be documented, kept up-to-date and approved by senior management.

The Company recognises that policies, procedures and controls may not always prevent and detect ML-TF. Nevertheless, a risk-based approach allows the Company to balance the cost of AML-CFT compliance resources with a realistic assessment of the risk of the Company being used in connection with ML-TF. A risk-based approach focuses resources and efforts where they are needed and where they have the greatest impact.

V. CUSTOMER DUE DILIGENCE

The Company shall apply Customer Due Diligence ("CDD") measures to a customer when it:

(a) establishes a business relationship with the customer;
(b) carries on an occasional transaction for the customer;
(c) suspects the customer of money laundering or terrorist financing; and
(d) doubts the veracity or adequacy of documents, data or information previously obtained for the purpose of identifying, or verifying the identity of, the customer.

The CDD measures that must be carried out involve:

(a) identifying the customer, and verifying his identity;
(b) identifying the beneficial owner, where relevant, and verifying his identity;
(c) assessing, and where appropriate obtaining information on, the purpose and intended nature of the business relationship or transaction.

Where the beneficial owner is a legal person, the Company must take reasonable measures to understand the ownership and control structure of that legal person.

For some business relationships, determined by the Company to present a low degree of risk of ML-TF, simplified due diligence (SDD) may be applied; in the case of high-risk situations, and specifically in relation to Politically Exposed Persons (PEPs), enhanced due diligence (EDD) measures must be applied on a risk sensitive basis.

Customer Screening:
When obtaining CDD or carrying on ongoing monitoring, the Company will perform searches against its customer's name, and against the names of the beneficial owners, controllers, beneficiaries etc. These searches can be performed using a wide variety of risk management systems or public domain searches.

When conducting searches against the name of an individual or entity, the Company shall consider "negative press" in addition to whether the individual or entity is named on a sanctions or PEP list. Negative press is the term given to any negative information, whether alleged or factual. This could be anything from an allegation of fraud by a disgruntled former customer to an article in a newspaper relating to a criminal investigation. Consideration will be given to the credibility of the information source, the severity of the negative press, how recent the information is and the potential impact the negative press would have on the business relationship with that customer.

The Company will document:
- the source and date of the search;
- actions taken to confirm or discount any potential match;
- details of the negative press;
- any actions taken to verify or disprove the claims; and
- any additional actions taken as a result of this information such as treating the customer as high risk and/or seeking proof of source of wealth/funds etc.

Simplified Due Diligence:
In general, the full range of CDD measures shall be applied by the Company. However, Simplified Due Diligence measures ("SDD") shall be implemented in cases where lower risks have been identified and where the CDD measures are commensurate with the lower risk factors. The following are examples of possible SDD measures that the Company may apply:
- verifying the identity of the customer and beneficial owner after the establishment of the business relationship;
- reducing the degree of ongoing monitoring and transaction monitoring, based on a reasonable monetary threshold in accordance with the customer's profile;

- relying on a third party to conduct verification of identity of the customer.

The possibility of applying SDD measures does not remove from the Company its responsibility to adopt CDD measures, it only allows for application of reduced measures. There may be instances, depending on the level of risk and all the known circumstances (a high-risk relationship e.g., PEPs will be dealt with more caution rather than the routine CDD measures), where it is inappropriate to adopt these SDD measures.

Under all circumstances, the Company must keep the customer risk assessment up to date and review the appropriateness of CDD obtained even if SDD measures are adopted. The Company shall keep the risk assessment and level of CDD requirements under review and the level of risk of the CDD measures should be consistent with the risk of the relationship.
The Company may apply SDD measures where lower risks have been identified and the SDD measures shall be commensurate with the lower risk factors. Where the Company decides to adopt the SDD measures in respect of a particular applicant, it must:

(a) document that decision in a manner which explains the factors which it took into account (including retaining any relevant supporting documentation) and its reasons for adopting the measures in question; and
(b) keep the relationship with the applicant (including the continued appropriateness of using the SDD measures) under review, and operate appropriate policies, procedures and controls for doing so.

SDD shall never apply where the Company knows, suspects, or has reasonable grounds for knowing or suspecting that a customer or an applicant for business is engaged in money laundering or terrorism financing or that the transaction being conducted by the customer or applicant for business is being carried out on behalf of another person engaged in money laundering or where there are other indicators of ML-TF risk. Where SDD measures are adopted, the Company shall apply a risk-based approach to determine whether to adopt the SDD measures in a given situation and/or continue with the SDD measures, although these customers' accounts are still subject to transaction monitoring obligations.

Enhanced Due Diligence:
The Company shall implement internal controls and other procedures to combat money laundering and financing of terrorism, including Enhanced Due Diligence ("EDD") procedures with respect to high-risk persons, business relations and transactions and persons established in jurisdictions that do not have adequate systems in place to combat money laundering and financing of terrorism.

Where the ML-TF risks are identified to be higher, the Company shall take EDD measures to mitigate and manage those risks. The Company must assign a high-risk rating to the applicant for business where a high risk of ML-TF has been identified. The EDD measures that may apply for higher risk relationships should include:

(a) requesting additional information on the customer and updating on a frequent basis the customer or the beneficial owner;

(b) obtaining additional information on the intended nature of the business relationship and the source of funds/wealth;
(c) obtaining information on the intended or performed transactions;
(d) obtaining the approval of senior management to commence or continue the business relationship;
(e) conducting close monitoring of the business relationship;
(f) any other measures the Company may undertake with relation to a high-risk relationship.

In case where the Company is unable to perform the required EDD requirements, it shall not commence or it shall terminate the business relationship and consider filing a suspicious transaction report.

Suspicious Activity Reporting:
Where a transaction is inconsistent in amount, origin, destination, or type with a customer's known, legitimate business or personal activities, the transaction shall be considered suspicious. Complex transactions or structures may have entirely legitimate purposes, however, the Company shall pay attention to all complex, unusual, large transactions, and all unusual patters of transactions, which have no apparent economic or visible lawful purpose. An unwillingness on behalf of a customer to provide the requested information is also grounds for suspicion.

All employees, regardless of whether they have a compliance function, are obliged to report to the Company's Anti-Money Laundering Compliance Officer ("AMLCO") each instance in which they have knowledge, suspicion or reasonable grounds for suspicion that funds or assets are criminal property or that a person in involved in ML-TF.

On receipt of a report concerning suspicious activity or customer, the AMLCO shall determine whether the information contained in such report supports the suspicion. The AMLCO shall investigate the details in order to determine whether in all the circumstances he in turn should submit a Suspicious Transaction Report ("STR") to the Belize Financial Intelligence Unit ("FIU"). If the AMLCO decides that the information does not substantiate a suspicion, he would nevertheless be required to record fully the reasons for his decision not to report to the FIU. Reporting STRs will allow the FIU to build a clearer picture of the ML-TF threat to Belize, and to use such intelligence on a proactive basis.

VI. ONGOING MONITORING

The Company must monitor its business relationships on an ongoing basis, which includes:

- scrutiny of transactions undertaken throughout the course of the relationship (including, where necessary, the source of funds) to ensure that the transactions are consistent with the Company's knowledge of the customer, his business and risk profile;
- determining whether the customer is a PEP;
- determining whether a customer relationship involves a country or territory that represents a higher risk for ML-TF, corruption, or being subject to international sanctions, including but not limited to, a country that has been identified by the FATF or CFATF (Caribbean Financial Action Task Force) as being higher risk;

- adjusting risk profiles and risk assessments based on information reviewed; and
- ensuring that the documents or information obtained for the purposes of applying CDD are kept up-to-date.

Up-to-date Record Keeping:
Documents or information obtained for the purposes of applying CDD measures, held about customers, must be kept up-to-date. Once the identity of a customer has been satisfactorily verified, there is no obligation to re-verify identity (unless doubts arise as to the veracity or adequacy of the evidence previously obtained for the purposes of customer identification) as risk dictates however, the Company must take steps to ensure it holds appropriate up-to-date information on its customers. A range of trigger events, such as an existing customer applying to open a new account or establish a new relationship, might prompt the Company to seek appropriate evidence.

VII. EMPLOYEE SCREENING

The Company shall implement programmes for screening procedures so that high standards are maintained when hiring employees. Employee screening shall be conducted at the time of recruitment, periodically thereafter, and where a suspicion has arisen as to the conduct of the employee.

Moreover, the Company shall ensure that its employees are competent and proper for the discharge of the responsibilities allocated to them.

VIII. ANTI-MONEY LAUNDERING COMPLIANCE OFFICER

The Company has appointed an Anti-Money Laundering Compliance Officer ("AMLCO"), whose principal functions are:

(a) to oversee and monitor the Company's compliance with the Belize AML-CFT laws, regulations, codes or guidelines being in force;
(b) receive and consider internal reports on unusual transactions and suspicious activities;
(c) consider whether a STR should be made to the FIU; and
(d) where he considers a STR should be made, submit the STR.

IX. INDEPENDENT AUDIT

The Company ensures that its AML-CFT policies, procedures and controls are objectively evaluated by a qualified and independent internal audit function. The main responsibilities of the audit function are to:

(a) assess the reliability, integrity and completeness of the Company's AML-CFT policies, procedures and controls;
(b) evaluate the Company's risk assessment processes and the risk ratings the Company has assigned with respect to its customers, business relationships, countries or geographic areas, services, delivery channels, products and transactions;
(c) assess the adequacy, accuracy and completeness of employee training and awareness programmes; and

(d) review the Company's past audit reports to assess the efficacy with which the Company has implemented previously recommended changes.

The audit is documented and retain in accordance with the Company's record keeping policies and procedures, and the results are reported directly to senior management and the Company's Board of Directors for timely action.

X. TRAINING

Programmes against money laundering and terrorism financing shall be in place to include ongoing training programme for the directors, officers, employees and contractors of the Company, to maintain awareness of the laws and regulations relating to money laundering and terrorism financing to:

(a) assist them in recognising transactions and actions that may be linked to money laundering or terrorism financing; and
(b) instruct them in the procedures to be followed where any links have been identified under paragraph (a).

XI. REVIEW OF THIS POLICY

The Company shall monitor the effectiveness of this Policy as part of its compliance monitoring programme. This Policy shall be reviewed periodically, and at least annually, to ensure it continues to meet the Company's compliance obligations and standards.

XII. APPROVAL OF THIS POLICY

The Company's senior management and Board of Directors has approved this Policy in writing as reasonably designed to achieve and monitor the Company's ongoing compliance with the requirements of this Policy. Any significant changes to this Policy shall be pre-approved by the Company's senior management and Board of Directors.