

BLACKWELL GLOBAL INVESTMENTS LIMITED

AML/CFT POLICY

**(Anti-Money Laundering and Countering Financing of Terrorism
Policy)**

TABLE OF CONTENTS

1.	Overview	3
2.	Scope and Objectives	3
3.	Money Laundering and Financing of Terrorism Definition	3
4.	Money Laundering Reporting Officer	3
5.	Customer Due Diligence	4
5.1	Ongoing CDD	4
6.	Suspicious Transaction Reporting	4
7.	Retention of Records	5
8.	Training	5
9.	General Internal Controls	5
	Appendix A – Customer Due Diligence Requirements	6

1. Overview

Being committed to the highest standards of the Anti-Money Laundering (“AML”) compliance and Counter-Terrorism Financing (“CTF”), Blackwell Global Investments Limited (hereinafter “Blackwell Global”, the “Company”), will maintain and enforce anti-money laundering procedures based on the anti-money laundering legislation of the British Virgin Islands.

The anti-money laundering legislation of the British Virgin Islands is contained principally in:

- the Proceeds of Criminal Conduct Act, 1997 (as amended) (the “PCCA”),
- the Anti-Money Laundering Regulations, 2008 (the “Regulations”),
- the Anti-Money Laundering and Terrorist Financing Code of Practice, 2008 (as amended) (the “Code”).

The Regulations and Code create mandatory requirements:

- to understand and verify the identity of the customers
- to maintain proper records of customer identification and verification, and business transactions for a minimum period of at least five (5) years; and
- to have internal controls and reporting procedures to ensure ongoing compliance, including the training of employees in the identification of suspicious transactions to prevent money laundering; and
- the appointment of a Money Laundering Reporting Officer (“MLRO”) responsible for continual compliance.

2. Scope and Objectives

The Policies are designed to establish a framework to:

- prevent Blackwell Global from being used, intentionally or unintentionally, by criminal elements for money laundering or financing terrorist activities;
- enable Blackwell Global to better understand its customers, their financial background and source of funds, to enable the Company to manage its risks prudently;
- put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws, procedures and regulatory guidelines; and
- equip employees with the necessary knowledge and training to deal with matters concerning AML/CTF.

Blackwell Global shall adopt a risk-based approach to AML/CTF. The risk-based approach encompasses identifying, assessing and understanding the money laundering (“ML”)/financing of terrorism (“FT”) risks to which Blackwell Global is exposed to, and to take measures proportionate to those risks for the purpose of mitigating them effectively. This implies that the degree, frequency and/or intensity of controls will be more comprehensive in situations assessed as posing a higher ML/FT risk, while these measures will be reduced in situations assessed as posing a lower ML/FT risk. However, it should be noted that situations assessed as posing a lower risk do not suggest that none or inadequate control measures will be applied.

3. Money Laundering and Financing of Terrorism Definition

Money Laundering (“ML”) is the attempt to conceal or disguise the nature, location, source, ownership or control of illegally obtained money. Money laundering is illegal. There are three stages of money laundering:

- a) Placement – introducing illegally obtained money into the financial system.
- b) Layering – disguising the audit trail to make it difficult to identify the original source of funds.
- c) Integration – transferring the ‘legitimate’ funds into a form which they can be used.

The financing of terrorism (“FT”) involves similar techniques to ML, to avoid detection by authorities and to protect the identity of those providing and receiving the funds.

4. Money Laundering Reporting Officer

The Money Laundering Reporting Officer (“MLRO”) is responsible for ensuring compliance by all employees with the relevant regulations and legislations. In addition, the MLRO also oversees the implementation of the policies and procedures as set out in this Policy, and resolving any matters or differences of opinion that may arise out of this Policy. Training will be

The MLRO is also responsible for reviewing the initial findings of unusual or suspicious transactions as reported by the management and employees, and assessing as to whether the described activities are genuinely suspicious which warrant a filing to the relevant authorities.

5. Customer Due Diligence

Customer Due Diligence (“CDD”) is the process through which Blackwell Global develops an understanding about its customers and the ML/FT risk they pose to the business. It involves the gathering and verifying of information about a customer’s identity, beneficial owners and any person acting on behalf of the customer.

Prior to the start of any business relationship, Blackwell Global will obtain documentary evidence of identity that includes a photograph (for individuals) and signature/s from all customers, corporate or individuals, and will ensure that satisfactory evidence is produced or such other measures that will produce satisfactory evidence of the identity of any customer or counterparty are taken. Blackwell Global will apply heightened scrutiny to customers, who are residents of countries as identified by credible sources as countries having inadequate AML standards or that may represent a high risk for crime and corruption, as well as to beneficial owners who resides in and whose funds are sourced from such named countries.

Unless the identity, the nature of business or formal requirements concerning the identification of the customer and/or beneficial owner(s) are known and fulfilled, Blackwell Global will not enter into, or maintain a business relationship with the customer.

Blackwell Global will request from all customers, including signatories to corporate accounts, the following information data to verify:

- full name(s);
- identification number or company identifier or registration number in the case of a company;
- date of Birth or date of Incorporation in the case of the company;
- nationality/citizenship or country of incorporation in the case of a company;
- residential address or registered business address in the case of a company;
- information relating the source of funds

In the case of a high money laundering risk profile, as assessed based on the customer’s jurisdiction, entity type and/or background, Blackwell Global reserves the right to request for additional information and/or documentations, without which there is no obligation to establish or maintain relationship with the customer after the periodic review.

Specific CDD documentation requirements for an individual and company are outlined in “Appendix A – Customer Due Diligence Requirements”.

5.1. Ongoing CDD

Ongoing CDD and account monitoring will be conducted to allow Blackwell Global to identify any inconsistencies between our existing knowledge of the customer and the transactions they undertake. Blackwell Global will review the information regularly, at least annually, to ensure that identify information is current and valid.

During the review, where it is noted that the customer’s circumstances change and it is deemed that insufficient CDD information is held, further information will be requested of the customer.

6. Suspicious Transaction Reporting

As a general rule, a suspicious transaction will often be one which is inconsistent with the customer’s known activities and profile or with the normal business expected for that type of client. Any transaction(s) other than a transaction (“Occasional Transaction”) occurring outside of a business relationship and that is over an applicable threshold value whether carried out in a single operation or several operations that appear to be linked, shall also be regarded as a form of suspicious activity.

Where a suspicious transaction has been detected and there are reasonable grounds to believe that a money laundering offence has been or is about to be committed, the Suspicious Transaction Report (“STR”) must be raised and completed by the Compliance and reported to the supervisory authority. Employees(s) may be disciplined if they fail without reasonable justification to report a potentially suspicious transaction.

An STR is the document that is used for reporting transaction(s) that is considered to be suspicious, that is, unusual or complex which includes, but is not limited to large transactions. The STR should also be used for those transactions that have no apparent economic or lawful purpose, although the value may be considered insignificant.

The STR or information relating to an STR must not be disclosed or provided to any person, other than a court, competent authority or other person authorized by law, that such information has been requested and/or furnished to the authority. It is a criminal offence for anyone, following the disclosure to the MLRO and/or the authority, to disclose or provide any information that might either “tip off” another person that a disclosure has been made or prejudice an investigation.

7. Retention of Records

Transaction records and data are maintained for a minimum period of at least five (5) years after the termination of the business transaction, namely:

- Business transaction records – to enable every transaction conducted to be readily reconstructed, so as to provide evidence if necessary, for the prosecution of criminal behavior;
- Identity and verification documents and information obtained during the CDD process and throughout the course of the relationship;
- Documentations related to money laundering topics, such as files on suspicious activity reports, findings of AML account monitoring, etc.

8. Training

Blackwell Global will maintain training programs to ensure that all employees are aware of their obligations in relation to ML/TF matters, the risks faced by the Company and how they should respond with faced with such risks. Training will be conducted periodically, no less frequently than once a year by the MLRO or an external provider, as arranged by the MLRO, and shall cover all aspects of this Policy, and the anti-money laundering and combating the financing of terrorism legislative provisions.

These training programs will equip employees with knowledge and understanding of new developments, money laundering and financing of terrorism techniques, methods and trends. It will also include their responsibilities relating to AML/ CFT, especially requirements relating to CDD, and the analysis of likely scenarios that may arouse suspicion which could result in an STR being generated.

Appropriate records of the training will be maintained and reviewed regularly by the MLRO to ensure that all employees have been adequately trained in their AML/CTF obligations.

9. General Internal Controls

It is prudent that Blackwell Global exercises extreme caution in dealing with individuals and corporate entities, including financial institutions from other countries, especially those that have no legal provisions or insufficient legal provisions to counter the incidence of money laundering.

Effective oversight and monitoring of the Policy must be in place to ensure continued compliance. The Policy will be audited by an independent auditor on an annual basis, and the report of the audit and review, together with any recommendations will be submitted to the Board of Directors for acceptance and approval.

Appendix A – Customer Due Diligence Requirements

Type	Documentation
Individuals	<p>1. Proof of Identity</p> <ul style="list-style-type: none"> • Passport • National ID Card • Driving Licence <p>The following must be ensured:</p> <ul style="list-style-type: none"> • The document bears the full name which corresponds to the name in which the customer account is being opened, the date of birth and identification number; • The document is valid and shows the issued and expiry dates; • The page bearing signature is included; • The copy is fully legible and the photograph clear and identifiable. <p>2. Proof of Residence</p> <ul style="list-style-type: none"> • Bank Statement • Utility bill – gas, electricity, water, landline, internet (excluding mobile and Wi-Fi subscriptions), TV/radio license/tax, council tax (or equivalent document, and/or notarized rental agreement). <p>The following must be ensured:</p> <ul style="list-style-type: none"> • The document bears the full name and full address which corresponds to the name in which the customer account is being opened; • The document is issued within six (6) months prior to the account application.
Corporate	<ul style="list-style-type: none"> • Certificate of Incorporation • Memorandum and Articles of Association • Certificate of Good Standing and/or Certificate of Incumbency • Shareholder and Director Registers • Audited Financial Statements • Resolution of the Board of Directors to open an account, and identification of those who have authority to operate the account and/or signatories to the corporate account • Full CDD documentation for each Directors and Shareholders (see “Individuals” above) • Full CDD documentation for each Ultimate Beneficial Owner owning more than 20% of the Company <ul style="list-style-type: none"> ▪ Where there are corporate shareholders, documentation confirming the identity of the Ultimate Individual Beneficial Owners must be provided.