Aureum
Trading Ltd

# POLICY AND PROCEDURES ON THE PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING

**JUNE 2021**

# Contents

## GLOSSARY OF TERMS USED IN THE POLICY

| | |
|---|---|
| **Affiliates** | Branches, subsidiaries or related parties of, or any entity that directly or indirectly controls, is controlled by, or is under common control with the Company |
| **AML** | Anti-Money Laundering |
| **Regulations** | Laws and Regulations of Malawi for combating ML, TF and other financial crimes |
| **CDD** | Customer Due Diligence |
| **CFT** | Combating the Financing of Terrorism |
| **CIBO** | Client Identification and Beneficial Ownership |
| **Clients** | Entities that have a commercial relationship with the Company |
| **Company** | Aureum Trading Limited, a private company incorporated under the laws of Malawi on 30 September 2019 with registration number TMBRS1011828 |
| **FATF** | Financial Action Task Force |
| **FIA** | Financial Intelligence Authority of Malawi |
| **FT** | Financing of Terrorism |
| **ID** | Identification |
| **INTERPOL** | International Police Organization |
| **IOSCO** | International Organization of Securities Commissions |
| **KYC** | Know Your Customer |
| **ML** | Money Laundering |
| **NID** | National Identification card |
| **STF** | Suspicious Transaction Form |
| **VR** | Verification |

## 1 INTRODUCTION

1.1. The combating of money laundering and the financing of terrorism has, in recent years, become a challenge of global proportions. Money launderers, terrorists and criminal groups have become more sophisticated in their methods and techniques.

For the purpose of this policy (the "**Policy**"):

**Money Laundering** is:

The process by which criminals attempt to conceal the true origin and ownership of the proceeds of criminal activities. If successful, the money can lose its criminal identity and appear legitimate. Criminals do this by disguising the sources, changing the form, or moving the funds to a place where they are less likely to attract attention.

**The Financing of Terrorism** is:

1) An offense within the meaning of the UN International Convention for the Suppression of the Financing of Terrorism (1999), where a person by any means, directly or indirectly, unlawfully and willingly, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out:

   (a) An act which constitutes an offence within the scope of and as defined in one of the treaties listed in the annex of the above-mentioned treaty, or

   (b) Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking any active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population or to compel a government or an international organisation to do or to abstain from doing an act.

2) For an act to constitute an offense set forth in paragraph 1, it shall not be necessary that the funds were actually used to carry out an offense referred to in paragraph 1, subparagraph (a) or (b).

1.2. The Government of Malawi, cognizant of the need for regulatory legislation, has enacted numerous laws at federal level to prevent and criminalize money laundering and the financing of terrorism.

1.3. The Company is legally obligated to establish a set of policies and procedures to ensure that its Clients and Affiliates do not engage in any activities that facilitate money laundering and/or the financing of terrorist activities. Section 15 provides a list of the laws applicable to this Policy.

## 2 THE COMPANY'S COMMITMENT

2.1. As a company registered under the laws of Malawi, the Company is committed to supporting both domestic and international efforts and initiatives aimed at combating money laundering and the financing of terrorism, in addition to implementing and enforcing such internal measures as may be deemed necessary.

2.2. The issuance of this Policy together with the implementation, operation, and enforcement of the procedures and controls therein, are a reflection of our commitment in this regard.

2.3. To combat money laundering and/or the financing of terrorism, the Company shall co-operate with FIA and international government agencies, and recognized law enforcement agencies.

## 3 POLICY CUSTODIAN

3.1. The top management of the Company shall be the appointed custodian of this Policy and shall be ultimately responsible for the implementation and enforcement of this Policy.

3.2. The compliance officer of the Company shall provide expertise and assistance regarding the implementation and enforcement of this Policy in order to properly support the top management of the company in properly discharging their duties.

## 4 PURPOSE AND RATIONALE

4.1. This Policy sets out the provisions, procedures and controls enacted by the Company concerning Anti-Money Laundering ("**AML**") and Combating the Financing of Terrorism ("**CFT**").

4.2. The rationale behind the Policy is unequivocally clear. The Company will only accept Clients whose sources of funds can be reasonably established as legitimate and who do not pose any risk (actual or potential) to the Company's reputation.

4.3. In light of the foregoing, the Company will not tolerate any involvement in illegal activities by its staff, Affiliates or Clients.

## 5 POLICY STATUS AND SCOPE

5.1. The provisions, procedures and controls detailed below are mandatory and shall apply to the Company's Clients, staff and Affiliates.

5.2. Breach of the Policy by any Client, staff or affiliate of the Company shall constitute a disciplinary offence and the Company reserves the right to take any additional action as it, in its sole discretion, deems fit in securing the diligent and proper implementation and enforcement of this Policy.

5.3. Suspension/reporting/termination applicable to Company's Clients, staff and Affiliates that are found to have violated the provisions of this Policy and process may include any or all the following:

- Warning;
- Temporary suspension of relationship;
- Termination of relationship;
- Reporting to the relevant authority (FIA or other competent authority as defined in the Financial Crimes Act No. 14 of 2017).

## 6 PROCEDURES AND CONTROLS (GENERAL)

6.1. This Policy contains, as an integral part to it, certain procedural checks and balances (collectively "**Procedures and Controls**"), so as to ensure the vigilant and effective operation of the Policy.

6.2. The Procedures & Controls are as follows:

- Identification, verification and know-your-customer ("**KYC**") measures;
- Updating of KYC information;
- Activity monitoring;

- Reporting of suspicious activities;
- Training and Awareness;
- Record Keeping;

and are dealt with in more detail in Section 8 below.

## 7 PERIODICAL REVIEW

7.1. This Policy shall be reviewed on at least an annual basis. Any review shall take into account legislative changes regarding AML and CFT and shall also examine the previous 12 months implementation of the Policy together with how such implementation may be improved. Any amendments made to the Policy under this section 7 must have received prior written sign-off from the Company's Top Management whereupon they shall take effect immediately.

## 8 IDENTIFICATION (ID), VERIFICATION (VR) AND KNOW-YOUR-CUSTOMER (KYC)

8.1. ID, VR, and KYC together form the first key step in the Procedures and Controls and is to be conducted prior to the establishment of a commercial relation with a Client. It enables basic background information about the Client, their business, source of funds and their expected level of activity to be obtained and an initial decision undertaken.

8.2. The carrying out of ID, VR and KYC procedures are mandatory.

8.3. In general, the Company accepts Clients that are legal entities, not physical persons. Where the Client is a company, the ID, VR, and KYC process must, in order to be valid, cover the following details regarding the Client company:

- Incorporated name;
- Shareholders (in case applicant company being non publicly traded);
- Names of Beneficial owners (in case applicant company being non publicly traded);
- Names of Managers/Directors;
- Signatories;
- Country of origin / UAE physical address (if applicable);
- Contact details;
- Previous business activities (type and volume);
- Anticipated type and volume of activities;
- Source of funds;
- Banking reference and introductory letter;
- Last two years audited financial statements;
- Details of external auditors.

The above list is a summary of the information required. A detailed checklist is attached in as Appendix A.

8.4. For individual person(s) (i.e. Beneficial Owners, Managers/Directors and Signatories), the ID, VR and KYC process must, in order to be valid, cover the following details regarding each individual Client:

- Full name (as per NID or passport);
- Date and place of birth;
- Nationality;
- Physical address (residential and business / home country and UAE);

- Contact details;
- CV;
- Source of funds (for Beneficial Owners);
- Bank reference letter (for Beneficial Owners).

The above list is a summary of the information required. A detailed checklist is attached in Appendix B.

### 8.5. KYC Process

8.5.1. KYC is to be carried out via the use of two (2) mandatory checklists:

- Corporate KYC Checklist (please refer to Appendix A); and
- Beneficial Owners / Managers / Directors KYC Checklist (Please refer to Appendix B).

8.5.2. The establishment of business relationship with shell companies is strictly forbidden. For the purposes of this section 8.5.2, a "shell company" shall mean an institution that has no physical presence in any country, and which merely exists on paper.

8.5.3. An integral part of the KYC process is the carrying out of Client screening and relative risk assessment. Screening ensures that a Client is not listed on those official sanctions lists issued by Government and departments and law enforcement agencies. The risk assessment process classifies the Clients into three risk categories: normal, medium and high. Clients classified under high risk, including applicants defined as Politically Exposed Persons – PEPs, shall be subject to enhanced CDD during both the approval and monitoring process and applications shall be submitted to senior management for approval.

8.5.4. When conducting the KYC process, no reliance must be placed on third party information or "hearsay" – ID, VR and KYC must all be carried out by the Company itself. Example, if a Client is introduced to the Company by a third party, the Company is still under a clear obligation to perform the ID, VR and KYC procedures.

8.5.5. It should be borne in mind that KYC is more than a procedure and is in fact a discipline that is to be encouraged and developed. For example, KYC should become second nature so that in addition to the foregoing, any significant information related to the Client obtained during meetings, telephone discussion, visits, press releases, etc. and which is deemed to be relevant for the purposes of this Policy should be recorded. Fresh CDD should be undertaken, especially if it appears that the veracity or accuracy of previous information is doubted.

8.5.6. The FATFA Guidance for Risk-Based Compliance for Designated Non-Financials Business and Professions – DNFBPs allows entities to adopt a risk-based approach to determine the extent of due diligence measures with the level of risk posed by the customer type, business relationship, transaction, product/service or geographical location. The list of documents mentioned in this Policy is not absolute or exhaustive and the Company should assess on a case-by-case basis what documentation and information is necessary and appropriate on each particular client.

## 9 KYC INFORMATION UPDATING

9.1. Reasonable steps must be taken to ensure that ID, VR and KYC information is updated as and when required. As a minimum standard, KYC information must be updated every 2 (two) years. For Clients that are considered of "high-risk", updating of CDD information should be performed on a yearly basis.

9.2. KYC updating is carried out via the use of those KYC updating checklists as attached in Appendices C and D.

## 10 ACTIVITY MONITORING

10.1. The Company is mandated to monitor, supervise and inspect the activities of its Clients and Affiliates.

10.2. As such, the activity monitoring will be undertaken in the form of inspections of Clients/Affiliates (desk and/or on-site, as the case require) to ensure that their operations are conducted in accordance with the AML Guidelines and Regulations.

## 11 REPORTING OF SUSPICIOUS ACTIVITIES

11.1. Article 23 of the Financial Crime Act. No. 14 of 2017 places a clear obligation on all Company staff and Affiliates to report any suspicious activities or information which may point to transactions, instructions, or arrangements related to illegal or unauthorized activities, with which any of its Clients is involved.

11.2. As such, it is the legal duty of Company's management, staff, and Affiliates to report any suspicious activity or information to the FIA (via a suspicious transaction report – "**STR**").

11.3. In doing so, it is important that:

- The reason for the suspicion is fully explained;
- No mention of the suspicion is made to the Client or any third party of the subject of the suspicion (failure to observe this requirement may result in the divulging party being prosecuted for the offence of 'tipping off'); and
- Any additional information as may be deemed necessary to conduct the investigation is furnished.

11.4. Any decision of the reporting institution to file a report to the FIA after receiving a STR, should be fully explained and the explanation should be recorded in the reporting institution's files.

## 12 TRAINING AND AWARENESS

12.1. Training shall be carried out at least once every two years for all relevant staff members, particularly for top management, so as to ensure that they are aware of those AML and CFT regulations, controls and responsibilities which require their compliance and which form the basis of this Policy.

12.2. Within one month of joining the Company all new staff members must be provided with an initial induction into the Policy, AML and CFT and the need for the reporting of suspicious transactions. Such induction may be carried out as part of the normal induction procedure.

## 13 RECORD KEEPING

### 13.1. KYC Documentation

For the purposes of this section 13, "KYC Documentation" shall refer to any information and documentation relating to Clients or entities which approached the Company for the purpose of establishing business relationship with, but for any reason such business relationship did not proceed.

### 13.2. Retention Periods

All KYC Documentation required under this Policy should be retained by the Company for a period of at least 5 years from the date of expiration/termination of a business relationship with a Client or 5 years from the date such documentation was obtained, whichever is the latest.

### 13.3. Investigations

Where a Client is the subject of an investigation of any kind, then all documentation relating to the investigation must be retained for such time until the authority conducting the investigation informs the Company otherwise in writing.

## 14 MANAGEMENT AND STAFF RESPONSIBILITIES

### 14.1. Scope of Responsibility

In carrying out the proper discharge of their duties under the Policy, both Company staff and management alike will be expected to:

- Undertake their due diligence role;
- Ensure their and their team's awareness of and compliance with ID, VR and KYC, record keeping and reporting;
- Undergo such ongoing AML/CFT training as the Company deems necessary from time to time;
- Ensure independency of the compliance function; and
- Support the compliance function.

## 15 REFERENCES

15.1. In this Policy reference has been made to the following legislation, directives and regulations (collectively the "**Regulations**"). In the event of any material change being effected to the Regulations following the date of this Policy coming into force, the Company shall make such amendments to the Policy as necessary to ensure that the intent, spirit and letter of the Regulation is reflected in the Policy.

- Financial Crime Act. No. 14 of 2017
- FATF 40 AML and 9 CFT Recommendations
- Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations

## APPENDICES

**Note:**

In the following Appendices, where a document is asked to be provided as an “authenticated” copy, then the copy must be authenticated as a true copy of the original by any of the following:

- Registered and practicing lawyer;
- Registered Notary Public;
- Chartered Accountant;
- Government ministry;
- Embassy or Consulate;

## APPENDIX A – CORPORATE KYC CHECKLIST

The following information/documentation must be collected and retained:

**A1** Proof of legal existence of applicant company:

- Trade License (if relevant in country of incorporation);
- Certificate of Incorporation; and
- Memorandum and Articles of Association.

**A2** Proof of applicant company's physical address in the country of origin and physical address within the UAE (when applicable):

- Utility bill; or
- Copy of lease/purchase agreement; or
- Original statement from a financial institution; or
- Letter from public authority or external auditor.

**A3** Contact details of applicant company:

- Office telephone number(s);
- Office fax number(s);
- Office email address; and
- Website address.

**A4** Names and addresses of all controlling individuals (managers/directors, shareholders and beneficial owners) of the applicant company (verified as per Appendix B, Sections B1 and B3).

**A5** Declaration by authorized signatories of the applicant company that the beneficial owners mentioned in A4 are the sole beneficial owners of the applicant company (in case of applicant company being non publicly traded).

**A6** Identities and addresses of all signatories of applicant company (verified as per Appendix B, Sections B1 and B3 if different to those at A4 above).

**A7** Identities and addresses, if different to those at A4 and A6, of:

- Individuals holding Powers of Attorney from applicant company; and
- Third party mandate holders of applicant company;

and verified as per Appendix B, Sections B1 and B3.

**A8** Understanding the relationship that exists between the principals of the applicant company and the powers of attorney/third party mandate holders.

**A9** Names and address of all partners in partnerships (verified as per Appendix B, Sections B1 and B3).

**A10** Details of applicant company's previous business including:

- Main products/services;
- Name and address of previous business;
- Main customers and suppliers;
- Main activities and geographical areas; and
- Volume of activities over last two years.

**A11** Indication of the anticipated volume and type of activity to be conducted by the applicant company.

**A12** Understanding the source of funds originating from the applicant company.

**A13** Bank reference whereby applicant company has been known to the issuing bank for at least two years.

**A14** Last two years audited applicant company financial statements.

**A15** External Auditors name and address, if company is subject to external audit.

**A16** For the purpose of this section A16, "Financial Intermediary" should be defined as an institution, firm or individual performing intermediation between two or more parties in a financial context such as banks, insurance companies, financial advisers, brokers or mutual funds.

For financial intermediaries only:

- Proof that the Financial Intermediary has been properly constituted, is supervised by a recognized authority and has good reputation.

If for any reason, any of the above documents cannot be obtained in original form, then they should be supplied as authenticated copies as per page 11.

## APPENDIX B – BENEFICIAL OWNERS / MANAGERS / DIRECTORS KYC CHECKLIST

The following information/documents must be collected and retained:

**B1** Valid, original ID card (for Malawi nationals) or passport clearly showing:

- Legal name (Change of Name Deed in the case of change of name);
- Date and place of birth; and
- Nationality

**B2** Proof of country of origin and physical address therein of individual in the form of:

- Passport; or
- Home country National ID; or
- Home country Driving license.

In those cases where the above forms of ID do not mention the Individual's physical address in their country of origin, this will need to be evidenced via those documents in B3.

**B3** Proof of individual's physical address in Malawi in the form of:

- Original utility bill; or
- Copy of lease / purchase agreement.

Where the individual is living at a temporary address, the details must be obtained and verified as per B3 above and an undertaking provided by the individual that they will advise the Company of the new permanent address once obtained. This should be followed up by the Clients Relations Dept.

**B4** Contact details of the individual:

- telephone number(s);
- Fax number(s); and
- email address.

**B5** Verification of contact details in B4 above via their testing by the Company.

**B6** Previous personal and business profile of each individual shareholder, such profiles to include previous occupations and/or types of businesses operated.

- Names and addresses of previous businesses or employers;
- Main products;
- Owners;
- Main customers and suppliers;
- Main activities geographical areas; and
- Volume of previous activities.

**B7** Indication of the anticipated volume and type of activity to be conducted by the individual's Applicant Company.

**B8** Understanding the source of funds (income, assets, net worth, etc) of each individual shareholder/manager.

**B9** Bank reference whereby the individual has been known to the Issuing bank for at least two years.

If for any reason, any of the above documents cannot be obtained in original form, they should be supplied as authenticated copies as per page 11.

## APPENDIX C – CORPORATE KYC UPDATING CHECKLIST

The following information/documents must be collected and retained:

**C1** Same year proof of physical address of Client in the form of:

- Original utility bill; or
- Copy of lease/purchase agreement.

**C2** Recent contact details of Client:

- Office telephone number(s);
- Office fax number(s);
- Office email address; and
- Website address.

**C3** Names and addresses of all new (since registration date or last update) beneficial owners and controlling individuals (Directors/Managers) of the Client (verified as per Appendix B, Sections B1 and B3).

**C4** Declaration by each Client's authorized signatory that the latest beneficial owners mentioned in C3 above are the sole beneficial owners of the Client.

**C5** Description of Client's activities (types and volume) for the last two years.

**C6** Client's audited financial statements for the last two years.

**C7** External auditors name and address.

## APPENDIX D – BENEFICIAL OWNERS / MANAGERS / DIRECTORS KYC UPDATING CHECKLIST

The following information/documents must be collected and retained:

**D1** Valid, original ID card (in the case of Malawi nationals) or passport clearly showing:

- Legal name (Change of Name Deed in the case of change of name);
- Date and place of birth; and
- Nationality.

If for any reason, any of the above documents cannot be obtained in original form, they should be supplied as authenticated copies as per page 10.

**D2** Same year proof of physical address of individual:

- Copy of utility bill; or
- Copy of lease agreement; or
- Copy of deed agreement.

**D3** Latest contact details of the individual:

- Telephone number(s);
- Fax number(s); and
- Email address.

## APPENDIX E – PRACTICAL ISSUES CONCERNING TRAINING AND AWARENESS (SECTION 12)

**E1** Any training provided under section 12 must include:

- An introduction into what is money laundering/financing of terrorism;
- Developing the ability to recognize suspicious activities or "early warning" signs (particularly regarding commodities trading);
- The requirements of local and international regulatory legislation and their ramifications; and
- This Policy.

**E2** Training and awareness can be raised through the following tools:

- Handbooks;
- Awareness messages;
- Courses (internal and external);
- Induction programs.

## APPENDIX F – PRACTICAL ISSUES CONCERNING RECORD KEEPING (SECTION 13)

### F1 Storage Location

If it is not possible or practicable (for example due to space constraints) to store KYC Documentation on site, then a suitable external location may be utilized. Suitable external locations may be:

- A secured area (e.g. warehouse, office) owned and/or operated by the Company or an Affiliate; or
- A secured area owned and/or operated by a reputable third-party provider.

Regardless as to whether KYC Documentation is stored on or off-site, the documents themselves must be stored in a secure, fireproof location such as a safe from a reputed manufacturer.

### F2 Use of Other Storage Media

As an additional safeguard, the Company should always maintain copies in secured electronic format and regular automatic backups should be performed.

### F3 Data Retrieval/Accessibility

The robustness of the security offered by any given storage option should not compromise the efficacy of data retrieval. Storage locations which prevent a reasonably fast retrieval of data should be disregarded in favour of suitable alternatives. The requirement for swift data retrieval is particularly important when dealing with third party conducted investigations where the Company may be requested to source and forward on data within a stipulated time period. As such, stored KYC Documentation should be indexed by reference to:

- Member name;
- Date stored;
- Data type (e.g. registration, license, correspondence, report); and
- details of the individual responsible for filing the KYC documentation in storage.