ANTI-MONEY LAUNDERING AND COUNTER-TERRORIST FINANCING POLICY – MCQUADE CONSULTING (UK) LIMITED

1. GENERAL PROVISIONS

1.1. This policy has been prepared by Thomas McQuade to set out the practice's policy for complying with the UK AML/CTF regime (principally, The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 ('the Regulations'), and the Proceeds of Crime Act 2002) . The practice is committed to upholding its AML/CTF obligations under UK legislation.

1.2. The Money Laundering Reporting Officer (MLRO) for this practice is Thomas McQuade.

1.3. Thomas McQuade must regularly review this policy (and in any case at least annually) to ensure it remains up-to-date and adequate. A written record must be kept of when the policy was last reviewed and any changes that were made.

1.4. This policy must be communicated and read by all staff. A written record must be maintained to confirm all staff have read and understood this policy. If any changes are made following the review set out in 1.3, these changes must also be communicated to staff and a written record maintained to confirm they have read and understood the changes.

2. PRACTICE RISK ASSESSMENT FOR AML/CTF PURPOSES

Example policy wording:

2.1. *A formal and documented practice risk assessment will be undertaken that will focus on the risk to the practice arising from factors including our clients, the countries in which we operate, the services we provide and how we deliver our services.*

2.2. The practice risk assessment will be renewed on a risk-sensitive basis and in any case at least annually.

2.3. From the most recent practice risk assessment, the key areas of risk to the practice at present are:

- *Cash from the proceeds of crime being laundered through legitimate businesses*
- *The proceeds of businesses being used in terrorist activities*

3. CLIENT DUE DILIGENCE (CDD) – CLIENT IDENTIFICATION

Example policy wording:

3.1. CDD must be carried out when the practice establishes a business relationship. To satisfy this, the CDD forms contained in CIMA's Members' Handbook will be used to:

- *Identify the client and verify their identity,*
- *obtain information on the purpose and intended nature of the business relationship,*
- *check for the existence of any beneficial owners, and, if present, identify them and take reasonable measures to verify their identity.*

3.2. The nature and extent of evidence and information obtained to satisfy 3.1 must reflect the level of risk the business relationship poses. Therefore the practice must perform a client risk assessment on every client to

assess the level of ML and TF risk they pose. To satisfy this, the CDD forms contained in CIMA's Members' Handbook will be used.

3.3. The requirements set out in 3.1 must be satisfied before a business relationship is established with the client. The only exception is where verification of the client (and, if applicable, any beneficial owner) is performed during the establishment of a business relationship because it is necessary to not to interrupt the normal conduct of business and there is little risk of ML and TF.

3.4. The practice's Terms of Engagement must outline the services to be provided with sufficient detail to make it clear to the client and our practice the intended nature and purpose of the business relationship and the services to be provided. The Terms of Engagement must also provide the client with the data protection information as required under regulation 41 of the Regulations.

3.5. The practice must not establish a business relationship if we have been unable to satisfy the requirements set out in 3.1 (as informed by the client risk assessment set out in 3.2). The practice must also consider making a suspicious activity report (SAR) to the MLRO (if applicable) or directly to the National Crime Agency (for example, if the client has been deliberately difficult or evasive). If a SAR is made, the practice must ensure it complies with its obligation to not tip off the client.

3.6. Should the client request additional or different services it may be necessary to perform all or part of the requirements set out in this section as necessary in relation to the additional or different services.

4. CLIENT DUE DILIGENCE (CDD) - ONGOING MONITORING OF CLIENTS

Example policy wording:

4.1. The practice must conduct ongoing monitoring measures, which includes:

- *scrutiny of transactions/activity undertaken throughout the course of the relationship (including, where necessary, the source of funds) to ensure that the transactions/activity are consistent with our knowledge of the client, the client's business and risk profile, and*
- *undertaking reviews of existing client records and keeping the documents or information obtained on the client up-to-date.*

4.2. The degree and nature of the ongoing monitoring measures in 4.1 must reflect the level of risk the business relationship poses (as identified in the client risk assessment set out in 3.2).

4.3. The practice must consider whether as part of the ongoing monitoring measures in 4.1 the level of risk the business relationship poses (as identified in the client risk assessment set out in 3.2) has now changed.

4.4. The practice must terminate the business relationship if we have been unable to satisfy the requirements set out in 4.1 (as informed by the client risk assessment set out in 3.2). The practice must also consider making a suspicious activity report (SAR) to the MLRO (if applicable) or directly to the National Crime Agency (if, for example, the client has been deliberately difficult or evasive). If a SAR is made, the practice must ensure it complies with its obligation to not tip off the client.

5. ENHANCED DUE DILIGENCE MEASURES (EDD)

Example policy wording:

*5.1. The practice must apply enhanced due diligence measures where any business relationship has been assessed as high risk in order to manage and mitigate the risk. EDD measures must be applied **in addition** to the requirements set out in 3.1 and 4.1. High risk situations include:*

a) a high risk of ML or TF as it is a high risk situation identified in our practice risk assessment and set out in 2.3 or in the information made available by our Supervisory Authority (CIMA),

b) the client is established in a high-risk third country,

c) the client is a politically exposed person, or a family member or known close associate of a politically exposed person (collectively referred to as 'a PEP'),

d) the client has provided false or stolen identification documentation or other information and we propose to continue to deal with that client,

e) a transaction is (i) complex and unusually large, or there is an unusual pattern of transactions, and (ii) the transaction or transactions have no apparent economic or legal purpose,

f) any other case which by its nature can present a higher risk of money laundering or terrorist financing, including a business relationship identified as high risk when we perform the client risk assessment set out in 3.2.

5.2. The CDD forms contained in CIMA's Members' Handbook will be used to assist with identifying whether any of the high risk situations set out in 5.1 apply.

***5.3.** Specifically in relation to identifying high risk situation 5.1 c), the practice has assessed that it is unlikely client will be a PEP. This is based on the practice risk assessment, the level of ML and TF the practice faces (and the extent to which that risk would increase should we establish a business relationship with such a PEP client), and the information made available by our Supervisory Authority (CIMA).*

In the absence of any factors that indicate the client may be a PEP, the practice will seek to identify such clients by asking them if they are a PEP and performing a web-based search.

5.4. The EDD measures the practice must apply for the high risk situations in 5.1 depend on the nature of the high risk, and may include:

- *seeking additional independent, reliable sources to verify information provided or made available to the relevant person,*
- *taking additional measures to understand better the background, ownership and financial situation of the client, and other parties to the transaction/activity,*
- *taking further steps to be satisfied that the transaction/activity is consistent with the purpose and intended nature of the business relationship,*
- *increasing the monitoring of the business relationship, including greater scrutiny of transactions/activity.*

5.5. Specifically for high risk situation 5.1 c), the practice must assess the level of risk the PEP client poses and the extent of EDD measures to be applied. When making this assessment, the practice must take into account information made available by our Supervisory Authority (CIMA) and HM Treasury approved guidance. However, EDD measures must at least include:

- *obtaining approval from senior management at the practice (if applicable) for establishing or continuing the business relationship with that client,*
- *take adequate measures to establish the source of wealth and source of funds which are involved in the proposed business relationship or transactions with that client; and*

- *where the business relationship is entered into, conduct enhanced ongoing monitoring of the business relationship with that person.*

5.6. Specifically for high risk situation 5.1 e), the EDD measures must at least include:

- *as far as reasonably possible, examining the background and purpose of the transaction, and*
- *increasing the degree and nature of monitoring of the business relationship in which the transaction is made to determine whether that transaction or that relationship appear to be suspicious.*

6. RELIANCE

Example policy wording:

6.1. The practice may rely on another regulated person under the Regulations to satisfy the requirements set out under 3.1, but the practice remains liable for any failure to satisfy these requirements.

6.2. If the practice relies on another regulated person, we must:

- *immediately obtain from them the information required to satisfy the requirements under 3.1., and*
- *enter into a written arrangement that (i) enables us to obtain from the regulated person immediately on request copies of any identification and verification data and any other relevant documentation related to the requirements under 3.1, and (ii) require the regulated person to retain copies of the data and documents referred to in (i) for the period of time required under the Regulations.*

7. APPOINTMENT OF MONEY LAUNDERING REPORTING OFFICER (MLRO)

Example policy wording:

7.1. The MLRO of the practice is Thomas McQuade.

7.2. Should the identity of the MLRO change, the practice must inform the supervisory authority (CIMA) of the identity of the new MLRO within 14 days of the appointment.

7.3. The MLRO is responsible for monitoring the adequacy of the practice's AML/CTF systems and controls and to mitigate and manage the risk of ML and TF.

7.4. The MLRO is responsible for ensuring all relevant employees receive AML/CTF training (as set out in Section 9).

7.5. Where an internal SAR is made to the MLRO, the MLRO must consider it in the light of any relevant information which is available to them and determine whether it gives rise to knowledge or suspicion or reasonable grounds for knowledge or suspicion that a person is engaged in money laundering or terrorist financing. If so, the MLRO must ensure that a SAR is made to the National Crime Agency.

8. SUSPICIOUS ACTIVITY REPORTING

Example policy wording:

*8.1. All staff must report knowledge or suspicion, or reasonable grounds for knowledge or suspicion, that another person is engaged in ML or TF ('suspicious activity'). This is a **personal obligation** for every member of staff and failure to report is a criminal offence punishable by imprisonment.*

8.2. The MLRO will make a suspicious activity report (SAR) to the National Crime Agency where required.

*8.3. The justification as to why a SAR was or was not submitted by the MLRO to the National Crime Agency will be recorded in a **confidential and separate place from the client file**.*

8.4. All staff must ensure the person on whom the SAR was made is not made aware of the SAR. It is a criminal offence punishable by imprisonment to disclose to a person that a SAR has been made on them.

9. TRAINING

Example policy wording:

9.1. The practice must:

- *make all relevant employees aware of the law relating to ML and TF, and to the requirements of data protection, which are relevant to the implementation of the Regulations, and*
- *regularly give all relevant employees training in how to recognise and deal with transactions and other activities or situations which may be related to ML or TF.*

9.2. Employees who are required to be provided with training under 9.1. are:

- *employees whose work is relevant to the practice complying with the Regulations, or*
- *employees whose work is capable of contributing to the identification and mitigation of the risk of ML and TF to the practice, or preventing or detecting ML and TF relating to the practice.*

9.3. The training provided must in particular focus on the key areas of risk identified in the practice risk assessment and set out in 2.3.

9.4. A written record of the training provided under 9.1 must be maintained and include the training content, the date of attendance, and employee confirmation that they attended and understood the training.

9.5. All relevant employees must receive the training provided under 9.1 upon joining the practice.

9.6. The MLRO is responsible for deciding when additional training is required or when training should be refreshed to satisfy the requirements under 9.1, and when doing so must take into account at least any changes in the nature of the practice, regulatory changes and whether any internal or external SARs have been made.

10. RECORD KEEPING

Example policy wording:

10.1. The practice must keep:

- *a copy of any documents and information obtained to satisfy our CDD (including ongoing monitoring and EDD) obligations set out in this policy,*
- *sufficient supporting records (consisting of the original documents or copies) in respect of a transaction (including an occasional transaction that does not form part of a business relationship) which is the subject of CDD (including ongoing monitoring and EDD) to enable the transaction to be reconstructed,*
- *suspicious activity records as set out in Section 8, and*
- *training records as set out in Section 9.*

10.2. The practice must keep the records set out in 10.1 for a period of 5 years. This will begin on the date on which the business relationship comes to an end (or for an occasional transaction that is not part of a business relationship, the date on which the transaction is complete).