Marvicap Limited

Anti-Money Laundering
And Countering the Financing of Terrorism
Policies and Procedures Manual

Document control

Version no.	Issue date	Issued by	Amendment - whole / partial
v1.0	October 2022	Paul Whelan	
V1.1	November 2023	Paul Whelan	
V1.2	May 2024	Paul Whelan	
V1.2	Dec 2024	Jo Stolk	Fixed spelling, etc.

Definitions

Business Risk assessment	The risk assessment which the business has undertaken to determine where it is vulnerable to the risk of money laundering or terrorist financing.
CDD	*See Customer Due Diligence*
CBC	*Central Bank of Cyprus*
Certification	The process by which copy documents, e.g. a passport copy, are independently verified to demonstrate that they are true copies of the original document.
CySEC	Cyprus Securities and Exchange Commission- Relevant AML/CTF Authority for the Republic of Cyprus.
Directive	The CBC has issued the 5th edition of the Directive on the Prevention of Money Laundering and Terrorist Financing ('the CBC AML/CFT Directive') based on (EU) 2018/849 of the European Parliament and of the Council (as amended), this Directive aims to combat money laundering by means of criminal law, enabling more efficient and swifter cross-border cooperation between competent authorities.
Customer Due Diligence ("CDD")	The term used to describe the identification and relationship information that we are required to collect as well as the verification documentation.
UBO Directors/Partners and Managers	Paul Whelan
Enhanced Due Diligence ("EDD")	EDD goes further than obtaining CDD. This involves considering whether additional identification information

	needs to be obtained, considering whether additional verification of identity is required, taking reasonable measures to establish source of wealth (in addition to source of funds) of the customer and beneficial owner and considering what ongoing monitoring of this information should be undertaken. EDD is to be undertaken when a new business relationship, occasional transaction, or a continuing business relationship is assessed as posing a higher risk of ML/FT, or when unusual activity is identified. When a suspicious activity is detected EDD should be considered.
FATF	Financial Action Task Force 5th Directive.
Gambling	The core principles to uphold are: • to keep the gambling industry crime free. • to protect the young and those at risk. • to ensure that the services offered by licence holders are fair and that players receive their true winnings.
Guidance	The EU's anti-money laundering and terrorist financing framework.
Legislative Framework and Laws	Cyprus AML Law in English regarding The Prevention and Suppression of Money Laundering Activities Law 40(I) of 2022; The Prevention and Suppression of Money Laundering Activities Law 98(I) of 2023.
MLRO	An individual to whom suspicions or knowledge of money laundering should be reported. This individual is Paul Whelan via parent company IMM Administration Limited.

Money Laundering Reporting Officer	*See MLRO.*
Politically Exposed Person	A customer who is exposed to the risk of bribery or corruption through the position that they hold.
Sanctions Notice	A Notice which requires that we do not do business with an individual or entity named in the Notice.
Source of Funds	Information about where the money has come from and who is paying it to us.
Source of Wealth	Information about the wealth of the customer and how this has been generated.
Terms of Business	An agreement which we put in place with an Introducer covering, amongst others, the responsibility for CDD.
Trigger event	An event which should prompt us to review the risk assessment of our customer and the CDD which we hold.

Section 1 - Introduction to the Manual

1.1 Purpose of the Manual

This Manual provides guidance on the procedures to be followed to best ensure that we comply with the various anti-money laundering and counter financing of terrorism requirements placed upon us and to assist you in understanding your personal obligations. This document is based on the Laws of the Republic of Cyprus with due regard to the European Union Directives of Anti Money Laundering and Counter Terrorist Financing. According to section 59(1)(a) of the Prevention and Suppression of Money Laundering Activities Laws of 2007 to 2023 ('the AML/CFT Law of the Republic of Cyprus')

1.2 Who does the Manual apply to?

This Manual applies to all staff and management of Marvicap Limited. There are no exceptions to this rule. Its contents have been approved by Paul Whelan.

This Manual should be followed at all times and non-compliance will be treated in an extremely serious manner.

If at any time it is impractical to follow the provisions of the Manual, written permission to deviate from the procedures must be obtained from Paul Whelan the **Money Laundering Reporting Officer ("MLRO")**, before any action is taken.

It should be read in conjunction with any guidance issued from time to time by the MLRO.

Whilst appropriate training will be provided on an ongoing basis, all staff must ensure that they are fully conversant with the underlying guidance. Copies of this documents are available from the **MLRO**.

If you are unsure as to how to apply any of these procedures or need more guidance as to your personal obligations, speak to the **MLRO**.

Failure to comply with the anti-money laundering or counter-financing of terrorism statutory requirements detailed in this Manual is a serious offence, which may result in your imprisonment and / or the imposition of a fine.

Failure to comply with Marvicap Limited`s internal Anti-Money Laundering procedures is also viewed seriously and could result in you being disciplined by Marvicap Limited.

1.3 Interaction with other procedures

Matters relating to Marvicap's other business policies and procedures are dealt with by Paul Whelan. This Manual applies in conjunction with these policies and procedures.

1.4 Appointment of a Money Laundering Reporting Officer ("MLRO")

Marvicap Limited ensures that a specific person is appointed to receive and analyse all internal reports and disclose any knowledge or suspicion of money laundering or terrorist financing to the relevant authorities. This person is commonly referred to as the MLRO and our MLRO is Paul Whelan. Paul Whelan is also appointed as Counter Financing of Terrorism Officer or CFTO. It is acceptable for this person to be the same person as the MLRO and so Paul Whelan fulfils this role as well.

1.5 Responsibility for updating this Manual

Paul Whelan is responsible for reviewing the contents of this Manual on an ongoing basis to ensure that procedural and / or regulatory or legislative amendments are reflected in the Manual.

1.6 Monitoring compliance with this Manual

The Guidance states that we must have procedures to ensure that we regularly monitor and sample test the implementation and operation of our anti-money laundering and counter financing of terrorism procedures and controls. Our compliance monitoring programme reviews compliance with our anti-money laundering and counter financing of terrorism procedures and the results of this monitoring are made available to the Board of Marvicap Limited.

The Guidance states that we must monitor and test how effective our anti-money laundering training has been. We do this through all staff attending annual AML training the results of which are input into our central training record. This record is held at the Marvicap office and provides evidence that staff have attended and understood their obligations in preventing money laundering.

Marvicap Limited will commission an annual report.

Section 2 – Background

2.1 What is money laundering?

Money Laundering is the process by which criminals attempt to conceal the true origin and ownership of the proceeds of their criminal activities. If successful, it also allows them to maintain control over these proceeds, to provide a legitimate cover for their source, and ultimately, enjoy the proceeds without being prosecuted. The requirement to launder the proceeds of criminal activities through the financial system is vital to the success of criminal operations.

2.2 Stages of money laundering

An effective money laundering operation will normally follow three stages:

- ***Placement*** of the criminally derived proceeds into the financial system, for example deposit into an account or as payment for goods or services.
- ***Layering*** by means of multiple transactions which separate the funds from their illegal origin by disguising or confusing the audit trail.
- ***Integration*** of the laundered money into the financial and business system with the appearance of legitimate funds or assets.

2.3 How we might be abused by money launderers

The main opportunities for identifying a money laundering operation occur in the placement and layering stages. These are the transactions that involve contact between the launderers and the business.

2.4 What is Terrorist Financing?

It is a criminal offence for someone to provide or collect funds that they know or suspect are intended for use to fund terrorist groups or acts of terrorism. Terrorist financing works slightly differently to money laundering, because the funds may derive from a legitimate source but are used for illegal acts. The process for disguising the destination of the funds is, however, similar to the way in which money launderers disguise the illegal origin of their funds.

Various Sanctions Orders have been issued by the United Nations concerning individuals and organisations that are believed to be involved in terrorist activities or the support of such activities. We have certain obligations in relation to checking whether any of our clients are named on the list.

Section 3 - Regulatory and legislative framework

3.1 Introduction

This Section summarises the main provisions of the anti-money laundering and counter financing of terrorism.

It is vitally important that you understand this Section because it explains your personal legal obligations under the current Anti-Money Laundering and Countering the Financing of Terrorism. It also details the penalties that you, as an individual, can incur if you do not adhere to the Anti-Money Laundering and Countering the Financing of Terrorism.

3.2 The legislation

The law relating to anti-money laundering and counter financing of terrorism is contained in Directive (EU) 2018/843 (the 5th anti-money laundering Directive). This is translated into Cypriot law the Prevention and Suppression of Money Laundering Activities Laws of 2007 to 2023 ('the AML/CFT Law').

CySEC's Directive for the Prevention and Suppression of Money Laundering and Terrorist Financing specifies the requirements for obliged entities (the 'Directive').

3.3 The Money Laundering and Terrorist Financing

The Money Laundering and Terrorist Financing directive places legal obligations on the directors, partners and managers of 'outsourced businesses' of Marvicap Limited.

In essence, Marvicap Limited ensures its Directors and Managers maintain:

- identification procedures;
- record keeping procedures (despite the Republic of Cyprus having two official languages Marvicap Limited elects to maintain all records in English);
- internal reporting procedures;
- internal staff screening procedures; and
- internal controls and communications procedures.

In order to comply, which has been developed to prevent Money Laundering and Terrorist Financing.

The Directors/Partners and Managers are also required to ensure employees are aware of the Anti-Money Laundering and Counter-Financing of Terrorism procedures that Marvicap Limited has in

place, which is the primary purpose of this Manual, and to arrange Anti-Money Laundering training including refresher training for all employees.

3.4 The key offences

All members of staff and management have personal obligations to ensure that we do not assist Money Launderers in any way. These obligations are summarised under the following key offences:

3.4.1 Assisting to retain

You commit the offence of assisting to retain if you enter into or become concerned in an arrangement which you suspect facilitates (by whatever means) the acquisition, retention, use or control of criminal property by or on behalf of another person. What this means in practice, for example, is that if you allow a customer to place funds with you when you have a suspicion that the funds might be criminal proceeds, you may be allowing that customer to retain criminal property.

You do not commit the offence of assisting to retain if:

1 You make a disclosure to the MLRO and you receive consent to continue with the business relationship or transaction; or
2 You have a reasonable excuse for not making the disclosure;

3.4.2 Acquisition, Possession or Use

You commit the offence of acquisition, possession or use, if you acquire, use or have possession of criminal property.

You do not commit the offence of acquisition, possession or use if:

1 You make a disclosure to the MLRO and you receive consent to continue with the business relationship or transaction; or
2 You have a reasonable excuse for not making the disclosure;

3.4.3 Concealing and Transferring

You commit the offence of concealing and transferring if you conceal, disguise, convert, transfer or remove criminal property from the Island.

You do not commit the offence of concealing and transferring if:

1 You make a disclosure to the MLRO and you receive consent to continue with the business relationship or transaction; or
2 You have a reasonable excuse for not making the disclosure;

3.4.4 Failure to Disclose

You commit the offence of failure to disclose if the following four conditions are satisfied:

1 You know or suspect or have reasonable grounds for knowing or suspecting that another person is engaged in money laundering; and
2 The basis of your knowledge or suspicion came to you in the course of regulated business; and
3 You know the identity of the other person or the location of the laundered property or you believe that you have information that will assist; and
4 You do not make a disclosure to the MLRO.

You do not commit the offence of failure to disclose if:

1 You have a reasonable excuse for not making a disclosure to the MLRO; or
2 You do not know or suspect that another person is engaged in money laundering and you have not been provided with anti-money laundering training as required.

3.4.5 Tipping Off

You commit the offence of tipping off if:

1 You disclose that you or another person has made a disclosure to the MLRO of information that became available through regulated business; and
2 Your disclosure is likely to prejudice any investigation which might come about as a result of the disclosure to the MLRO;

You also commit the offence of tipping off if:

1 You disclose that an investigation is being contemplated or is being carried out; and
2 Your disclosure is likely to prejudice that investigation.

3.4.6 Terrorist property

You commit an offence if you enter into or become concerned in an arrangement which facilitates the retention or control by or on behalf of another person of terrorist property.

You do not commit an offence if you did not know or had no reasonable cause to suspect that the arrangement related to terrorist property.

3.4.7 Prejudicing an investigation

You commit the offence of prejudicing an investigation if you know or suspect that an appropriate officer is acting (or proposing to act) in connection with a confiscation investigation, a civil recovery investigation, a detained cash investigation or a money laundering investigation and you:

1 Make a disclosure which is likely to prejudice the investigation; or
2 You falsify, conceal, destroy, or otherwise dispose of or cause or permit the falsification, concealment, destruction or disposal of documents which are relevant to the investigation.

You do not commit the offence of prejudicing an investigation if:

1 You do not know or suspect that the disclosure is likely to prejudice the investigation; or
2 You do not know or suspect that the documents are relevant to the investigation or you do not intend to conceal any facts disclosed by the documents from an officer carrying out the investigation.

3.5 The approach

In determining our compliance with our responsibilities, it is very important that our procedures reflect, as much as possible, the requirements of the Directives and domestic Cypriot Legislation giving effect to those Directives and the regulations imposed by CySEC.

Indeed, the key to the prevention and detection of money laundering and terrorist financing is the establishment of, and strict adherence to, effective systems and controls which include sound customer due diligence procedures based on international standards. CySEC has also stated that it will consider the extent of compliance with the Directive when conducting its supervisory visits, therefore, it will be directly relevant to its status and any assessment of the fitness and propriety of its principals.

This covers the following areas:-

- Corporate Governance, Vigilance, Systems and Controls;
- Know Your Customer and Customer Due Diligence;
- Identification and verification of identity;
- Ongoing monitoring of business relationships and recognising suspicious transactions and activity;
- Reporting suspicious transactions and activity;
- Vetting, awareness raising and training of employees; and
- Record Keeping.

3.6 The Financial Action Task Force ("FATF") http://www.fatf-gafi.org/

The FATF is the collective name for a group of countries who have established a common set of standards aimed at preventing money laundering. The member countries of the FATF are required to adopt these. The FATF member countries have been included in the list of the countries which are considered to have equivalent anti-money laundering requirements.

3.7 Sanctions Notices

Marvicap Limited recognises as part of its AML/CFT framework that if terrorist financing is detected with reference to sanctioned screening, then the funds are automatically frozen and reported to the MLRO. Marvicap Limited refers to sanctions resources that are available including OFAC list, United Nations list and the European Union List.

The MLRO is registered for updates to the financial sanctions website and the updated sanctions list is noted to the technical officer who will cross reference sanctioned names against new customers, focusing upon the regime list.

Once identified the sanctioned customer`s account will be frozen and the individual will be reported to the MLRO for action.

The United Nations issues resolutions from time to time which place obligations on its member states. In September 2001, the UN issued a Resolution in relation to freezing the funds of entities and / or persons suspected of committing, or posing a significant risk of committing, or providing material support for acts of terrorism.

The MLRO is responsible for ensuring that we meet the requirements in relation to **all** Sanctions Notices and for taking appropriate action as required.

3.8 Bribery

Marvicap Limited operates under the following provisions of the laws of the Republic of Cyprus:

- The Prevention of Corruption Law, Cap 161 of 1920 as amended by Law 97(1)/2012
- The Civil Servants Law of 1/1990 which governs the conduct of civil servants in general. It makes specific provision regarding bribery of public officials at sections 69 and 70
- The Law Sanctioning the Criminal Law Convention on Corruption No. 23(III) of 2000 (Law No. 23(III) of 2000) and Law 22(III) of 2006

Bribery includes four offences:

1. Requesting a bribe;
2. Receiving a bribe;
3. Bribing a foreign/domestic public official; and

4. Failing to prevent bribery.

The fourth offence is a corporate offence and the only defence to it is that the company had adequate anti-bribery procedures in place. Further information on such procedures will be communicated to you by Paul Whelan.

Section 4 – Business Risk Assessment

4.1 Business Risk assessment

Marvicap Limited undertakes an assessment of how vulnerable our business is to money laundering and terrorist financing so that we can address the risks of being used by criminals through appropriate procedures and controls. We need to record and document our risk assessment and we also need to keep it updated.

In undertaking our risk assessment, we have considered the following categories of risk:

- **Organisational Risk** – this includes the countries in which we do business, the types of monetary transactions that we enter into, our business volumes and whether we outsource any aspect of our regulated activities.

- **Customer Risk** – this centres around the types of customer that are likely to pose a higher risk for our business.

- **Business Risk and Product or Service Risk** – this centres on how likely it is that a money launderer or someone engaged in terrorist financing would use our products and services for that purpose.

- **Delivery risk** – this is about how we deliver our product or service to our client. For example, if we never meet our client and our relationship with the client is conducted remotely, this could be considered as higher risk.

Our business risk assessment has been undertaken by Paul Whelan. It will be reviewed on an annual basis. We are under an obligation to revisit our risk assessment if we start to do anything new which could impact upon it. Paul Whelan will be primarily responsible for this but if there is anything which you consider affects our business risk assessment, please discuss this with Paul Whelan.

4.2 How does the Business Risk Assessment affect our new customers?

Those aspects of our business and our customers which we consider attract a greater level of risk are called 'risk hot spots'. If any of our customers touch a risk hot spot, we will class that customer as high risk and we will require enhanced due diligence. To assist you in identifying whether a customer touches one or more risk hot spots, you should risk assess each customer. The customer

will either be classed as low risk or higher risk and this will determine the level of customer due diligence you require.

It is important that you complete the risk assessment to the best of your ability and that you pass it on to Paul Whelan for review and sign-off. You will be expected to obtain customer due diligence in line with the risk assessment.

4.3 How is the Business Risk Assessment affected by technological developments?

Marvicap Limited has procedures and controls in place to prevent the misuse of technological developments for the purpose of money laundering and terrorist financing. What this means in practice is that we must understand what new technologies money launderers are using and consider the risks to our business as a result. Paul Whelan is responsible for maintaining an awareness of the technologies and methodologies being used by criminals and he will do this by continual monitoring and discussions with IT when required. If Paul Whelan considers that there are implications for our business, it is his responsibility to review the business risk assessment.

Section 5 – Customer Due Diligence

5.1 Introduction

This Section will explain what customer due diligence you are required to get for customers who are classed as standard risk and what else you need to get for customers who are classed as higher risk. Customer due diligence will be broken down into identification information, relationship information and verification for individuals, trusts and legal persons. We will then discuss procedures for Acceptable Applicants, recording Customer Due Diligence, Source of Funds and Source of Wealth, Politically Exposed Persons and Introducers.

We must generally complete our CDD procedures before we commence the business relationship, however due to the small transaction sizes of a majority of our payments we have thresholds in place, where, when exceeded the appropriate verifications will take place.

The thresholds that once breached that trigger a customer verification.

- **Customer is over the age of 75**
- **Deposit greater than €350 or equivalent**
- **More than one deposit greater than €350 or equivalent in a calendar month**
- **On payout of any winnings**

It is important to note that if we cannot fulfil our CDD obligations, then we cannot proceed with the business relationship. In such instances, the matter should be referred to The MLRO and you should consider your suspicion reporting obligations in line with this

Manual. This is regardless of whether a transaction has actually taken place.

Enhanced Due Diligence ("EDD") – as per The Central Bank of Cyprus which has issued the 5th edition of the Directive on the Prevention of Money Laundering and Terrorist Financing ('the CBC AML/CFT Directive

If this paragraph we must:

(a) consider whether additional identification data needs to be obtained;
(b) consider whether additional aspects of the participant's identity or the identity of the business participant need to be verified;
(c) take reasonable measures to establish the source of any funds and of the wealth of the participant and any beneficial owner and underlying principal; and
(d) consider what on-going monitoring should be carried on.

5.2 What are the Customer Due Diligence requirements for individuals?

The following sections explain the identification and relationship information we require for all individuals. They explain what additional information we need for high risk individuals and the ways in which we can verify the identity and address of individuals. There is also some guidance on what to do if an individual cannot provide standard identity or address verification.

5.2.1 Identification information for individuals

We need to collect the following for all individuals:

- Legal name;
- Permanent residential address, including postal code;
- Date and Country of birth;
- Nationality;
- Gender

We will collect this information on account opening and we will record it in the CRM.

ONCE WE HAVE COLLECTED ALL OF THE ABOVE INFORMATION, WE WILL RISK ASSESS THE INDIVIDUAL. Please note that we keep all records in English.

5.2.2 Identification information for higher risk individuals

Where we have rated an individual associated with the relationship as higher risk, we need to collect the following:

- Details of any public or high profile positions held.

If the individual does hold a public or high profile position, there are additional requirements which you must follow.

5.2.3 Verification of an individual's identity

We are required to verify the identity of each individual associated with the relationship by obtaining one of the following for each individual:

- Current valid full passport bearing the individual's photograph;
- Current national identity card bearing the individual's photograph;
- Armed forces identity card bearing the individual's photograph; or
- Current valid provisional or full driving licence bearing the individual's photograph

It is important that you check that the verification document you obtain is current and valid and that it matches the information we have collected as mentioned above.

5.2.4 Verification of an individual's address

We are required to verify the address of each individual associated with the relationship by obtaining one of the following for each individual:

- Photographic driving licence or national identity card containing the current residential address only if the document has not already been used to verify identity;
- Correspondence from an official independent source such as a central or local government department or agency;
- A recent rates, council tax or utility bill (which must not be more than six months old);
- A recent account statement (no more than six months old) from a recognised bank, building society or credit card company; or
- The most recent mortgage statement from a recognised lender.

We will not accept a non-residential address for an individual. Where the individual provides us with a care of address, we will only accept this if we have a full and clear explanation for it signed by the individual and we know how long the individual expects to be at this care of address. All care of addresses must be signed off by Paul Whelan prior to the completion of our Customer Due Diligence procedures. The MLRO will be responsible for monitoring all customer relationships with care of addresses and to facilitate this monitoring, all such relationships will be logged in Client Relationship Management ("CRM").

5.3 Am I permitted to provide services to the client before Customer Due Diligence is complete?

Marvicap Limited accepts that, in exceptional circumstances where there is little risk of money laundering or terrorist financing, the verification of the identity of an applicant for business can take place after the business relationship commences provided the following criteria are met:

- The verification is completed as soon as reasonably practicable;
- It is essential that the services are provided before the Customer Due Diligence is complete;
- The risk of money laundering or terrorist financing is being effectively managed;
- The amount, type and number of transactions must be limited and monitored; and
- Senior management sign off is obtained on the commencement of the business relationship and on any subsequent activity until the Customer Due Diligence is complete.

Where it is considered that the business relationship should commence before the Customer Due Diligence is complete, this must be signed off by The MLRO. The file must be marked as 'CDD incomplete' and all significant interaction with the client must be also referred to the same person who signed the incomplete CDD off originally for further sign off. **It should be noted that if the client is assessed as higher risk, CDD must be completed before services are provided to the client.**

5.4 How do I record evidence of Customer Due Diligence?

The Customer Due Diligence information and documentation that we collect and record must be a good quality photocopy but in some cases we may ask for it to be provided in either the original form or in certified copy form.

.

Where we have not met one or more of the parties to the relationship, we will generally be unable to determine that the documentary evidence collected actually relates to that party. For this reason, we will expect to obtain certified copy documents from parties that we have not met.

If we have any doubt about the authenticity of the certified documents or about whether the documents relate to our customer, there are further checks that we must undertake.

5.5 What are the requirements in relation to Source of Funds and Source of Wealth?

5.5.1 Source of Funds

In order to complete a compliant risk assessment of a participant or business participant, a licensee must establish their source of funds. For a participant, the source of funds is likely to be their debit card. For a business participant, the source of funds is likely to be a bank account in the business participant's name. Marvicap Limited would expect the risk profile to increase if a payment

mechanism were used which did not require customer due diligence procedures to be implemented prior to the mechanism being made available.

5.5.2 Source of Wealth

Information sufficient to establish the source of income or wealth should be obtained for all higher risk relationships and all other relationships where the type of product or service being offered makes it appropriate to do so because of its risk profile. The source of wealth means how the customer has generated his/her overall wealth which is enabling him/her to establish a relationship with us. What we are seeking to establish by determining the source of wealth is whether the wealth of the customer is legitimate or if there is anything about it which might warrant further enquiries.

Marvicap Limited requires that reasonable measures are undertaken to establish the source of wealth of participants that have been assessed as posing a higher risk of ML/FT or are the subject of unusual or suspicious activity. A licensee should consider whether enhanced due diligence (which includes establishing source of wealth) should be undertaken when a participant attempts to make a qualifying payment.
Source of wealth is distinct from source of funds and describes the origins of a person's financial standing or total net worth (i.e. the activities that generated a person's funds and property). What constitutes "reasonable measures to establish" will vary depending on the level of risk associated to the participant or business participant and the activity seen. Effort should be made to obtain information that can be verified. For example rather than simply "salary" a participant should be asked for their employer name and position held. This could be verified, if necessary, by obtaining a pay slip or undertaking public domain searches.

5.6 What are the requirements for Politically Exposed Persons?

5.6.1 What is a Politically Exposed Person?

Politically Exposed Persons Risk or "PEP" risk relates to the risks associated with providing financial and business services to government ministers or officials from countries with widely-known problems of bribery, corruption and financial irregularity within their governments and society. The definition of a PEP extends also to the immediate family and close associates of such government ministers or officials. This risk is even more acute where such countries do not have adequate anti-money laundering standards, or where these do not meet international financial transparency standards. Our business could face considerable reputational damage if we were found to have a business relationship with clients involving the proceeds of corruption.

5.6.2 What are our procedures in relation to Politically Exposed Persons?

Marvicap Limited has procedures in place to apply enhanced due diligence to PEPs.

To determine whether any party associated with a relationship is a PEP, we will check every party against Public and propriety databases. This is regardless of whether the party has advised us of any public or high profile positions which they hold. We will record the results of our checks in a PEP register.

Where we identify through our checks that a party is a PEP, we will conduct enhanced due diligence by obtaining Relevant information Enhanced Due Diligence ("EDD") and the relationship will be treated as high risk. Once the EDD has been completed, the matter will be passed to The MLRO for review and approval and details will be added to our PEP register.

Paul Whelan will assign someone to be responsible for reviewing this register on an annual basis and for reviewing the associated client files in order to determine whether we require any additional information or documentation.

5.6.3 How do our procedures relate to our existing clients?

We may find that we become aware, through press coverage for example, that an existing party to a relationship has acquired PEP status. If this is the case, you should refer the matter immediately to The MLRO who will advise you as to what steps we need to take to ensure that we follow the procedures.

Section 6 - Monitoring

6.1 Introduction

Marvicap ensures monitoring of the conduct and activities of our client relationships in order that we can identify anything which is out of step with what we know about the relationship or those associated with it.

If we do not carry out ongoing monitoring, we risk not being able to identify if any of the parties associated with a relationship are utilising that relationship for money laundering or terrorist financing purposes.

We conduct our monitoring on an ongoing basis and we also take the opportunity to review our client relationships on the occurrence of certain trigger events. This Section will explain to you the ongoing monitoring that we conduct as well as the specific trigger events which we use to review our Customer Due Diligence information and documentation. Guidance is also given as to our procedures for complex, large or unusual transactions.

6.2 Ongoing monitoring

Questions you should ask yourself when dealing with any transaction for any client include:

- Is the nature and type of the transaction what we would expect for this client?
- Is the amount of the transaction in keeping with what we would expect and with the other transactions which have been carried out for this relationship?

Where a relationship has been classed as higher risk, our ongoing monitoring is more formal and we will review each high risk relationship on an annual basis. Paul Whelan will be responsible for conducting such reviews and the results. Any recommendations to obtain additional documentation and information will form part of the results of the review and Paul Whelan will be responsible for ensuring that this is obtained as well as for reporting progress. In the event that additional documentation or information is not forthcoming, we will be required to withdraw from the business relationship and this will be handled by Paul Whelan.

6.3 Trigger events

In addition to the ongoing monitoring which we carry out, we will review the Customer Due Diligence that we hold on the occurrence of certain trigger events. This is regardless of the risk categorisation of the customer. The trigger events that you are required to look out for include:

- A change in an existing client's personal circumstances;
- A change to the activity of the client;

- Changes to the nature, volume or size of transactions undertaken.
- Any customer who is aged over 75 years of age

Where any of these events happen, you are required to review the Customer Due Diligence information we hold and discuss any further information or documentation that you think we require with the MLRO. In the event that additional documentation or information is not forthcoming, we will be required to temporarily block the client relationship and this will be handled by the MLRO.

6.4 Complex, large or unusual transactions

Marvicap Limited will ensure transactions are reviewed, which are complex, large or unusual and which are not in keeping with what we know about our customer. Where we consider that a transaction is complex, large or unusual, we are required to examine the purpose and background of the transaction to ensure that we are comfortable with it. If you consider that a transaction is complex, large or unusual for the customer, you must refer it to Paul Whelan as soon as possible. Customer Services will be responsible for liaising with the customer to understand the transaction and to determine whether additional Customer Due Diligence is required. The MLRO will also be responsible for keeping the appropriate records. In the event that additional documentation or information is not forthcoming, we will be required to withdraw from the business relationship and this will be handled by the MLRO.

6.5 Impact of monitoring on risk assessment

Where our monitoring, either ongoing or on a trigger event, identifies significant changes in what we know about our customer, we must revisit the risk assessment we have carried out for the customer to determine whether the risk categorisation has changed. The MLRO will be responsible for reviewing the risk assessment and for determining whether the risk categorisation has changed. Where a customer is classed as high risk as a result of our monitoring, Customer Services will be responsible for liaising with the client to obtain the additional Customer Due Diligence that we may require. The customer will also be entered into our high risk log and any additional parties to the relationship will be assessed to determine whether the revised risk categorisation impacts on them. In the event that additional documentation or information is not forthcoming, we will be required to withdraw from the business relationship and this will be handled by the MLRO.

Any additional information or documentation which we obtain as a result of our monitoring must be retained on our customer files. This includes notes of any meetings, discussions or telephone calls that are held with the client as a result of any changes identified.

6.6 Impact of monitoring on existing customers

If any of our monitoring methods identify that we have not yet risk assessed the customer or we have not obtained Customer Due Diligence information or documentation, we must risk assess the customer and obtain Customer Due Diligence as if they were a new customer.

6.7 Dealing with unreasonable customer instructions

We are aware that customers can sometimes structure transactions so that the economic purpose of the transaction is obscured or to avoid currency transaction reporting requirements in some jurisdictions. Where we do not understand why a customer is asking us to structure a transaction in a certain way, we are required not to just comply with customer instructions in case we are facilitating money laundering. Where you do not understand why a customer wants a transaction to take place in a certain way, it is imperative that you discuss the situation with the MLRO. Records to support compliance with the customer's instruction or otherwise must be retained on the client file and we must document on the client file whether the instruction has had any impact on the risk rating of the customer. Where you have a suspicion as a result of the instruction, you must follow the procedures in Section7 in relation to reporting your suspicion.

Section 7 – Recognition and reporting of suspicions

Marvicap Limited ensures that sufficient guidance must be given to staff to enable them to form a suspicion or to recognise when money laundering or terrorist financing takes place. Section 5 of this Manual explains the information and documentation that we collect to make sure that we know enough about our customers. Section 6 explains how we monitor against that information to determine whether there is anything which we need to be concerned or suspicious about. This Section will provide you with further assistance about the recognition of suspicious activities and what you should do to report your suspicions.

7.1 What is a suspicious activity?

Quite simply, a suspicious activity will often be one which is inconsistent with a client's known, legitimate business or personal activities or with the normal business for that type of client and which may prompt a suspicion of money laundering.

7.2 Examples of suspicious activity

Typically, suspicious activities are those that appear to have no sound commercial reason or which do not constitute the most logical, convenient or secure way to do business.

Some examples of potentially suspicious activities are as follows:

- Transactions, instructions or activity that are unnecessarily complex;
- Where the transaction being requested is out of step with the normal transactions for the customer or is outside the normal scope of business that we conduct;

- Where the size or pattern of transactions is out of keeping with what has happened before or what we thought was going to happen;
- Where the customer is reluctant to provide us with information or documentation that we have requested;
- Where the customer wants to terminate the business relationship within a short time of commencing it, particularly where this involves the return of funds;
- Connections with high risk jurisdictions;
- Unnecessary routing of transactions through third parties.

7.3 How can we assess suspicious activity?

Marvicap Limited suggests some factors that should be borne in mind when seeking to identify a suspicious transaction or instruction and some of these are detailed below.

- Is the client known personally?
- Is the transaction in keeping with the client's normal activity?
- Is the role of any agent involved in the arrangement unusual?
- Is the transaction to be settled in the normal manner?
- Are there any other transactions linked to the transaction in question which could be designed to disguise money and divert it into other forms or to other destinations or beneficiaries?
- Are the reasons for the transaction transparent and understandable i.e. is there an easier, cheaper or more convenient method available?

7.4 Reporting suspicions

7.4.1 Why do we have to report suspicions?

It is an offence to fail to disclose where a person knows or suspects or has reasonable grounds for knowing or suspecting that a money laundering or terrorist financing offence has been committed. It is, therefore, vital that you report any suspicions or knowledge of money laundering or terrorist financing that you have. This includes instances where no transaction actually takes place or where no business relationship is formed.

7.4.2 How to report suspicions and / or knowledge of money laundering or terrorist financing

When you have a suspicion or knowledge of money laundering or terrorist financing, you **must** report it immediately. Whilst you are permitted to discuss the situation with your manager in advance of making a report, if you are still suspicious, you still have an obligation to report. It is vital that you do not discuss the situation with anyone else as you may commit the offence of tipping off.

All suspicions should be reported to the MLRO who is Paul Whelan, using the **"Suspicion Reporting Form"**. This will then be reported to CySEC.

Upon receipt of this form, the MLRO will issue you with an acknowledgement of receipt of the report which includes a reminder about not tipping off. You should keep this receipt in a safe place as it is documentary evidence that you have complied with the requirement to report any suspicions you may have. Do not place the receipt on any client file, introducer file or any other file that is used by staff members generally. This is to ensure that no one else is aware of the fact that you have made a suspicion report and that therefore no one can "tip-off" the client. The offence of tipping off is explained in Section 3.

It is very important that you wait for consent from the MLRO before undertaking any transaction which relates to a suspicious transaction report that you have made. The MLRO will advise you of consent by email. It is vital that this consent is kept confidential to you in order to avoid the offence of tipping off.

It is important to remember that the offences described in Section 3 relate to each suspicion that you have so each time you are suspicious, you should make a report to the MLRO.

7.4.3 What happens after a report is made?

The MLRO is obliged to consider any reports in the light of all relevant information available to him for the purpose of determining whether or not it gives rise to a knowledge or suspicion of money laundering.

To demonstrate the conclusions reached in relation to each suspicious transaction report, the MLRO must retain records which show the assessment of the report and the decision reached. These records are kept in the internal disclosures register which is confidential to the MLRO.

The fact that a suspicious transaction report has been made may impact on the risk assessment of the customer. As part of his considerations, the MLRO will, therefore, consider the impact on the risk categorisation. If the client is assessed as being higher risk, the client will be added to the high risk register and the MLRO will liaise with Customer Services to ensure that additional due diligence is undertaken. It will be vital in this situation to handle the relationship with the client sensitively to avoid tipping off and these situations will, therefore, always be handled by the MLRO.

7.4.4 Recording the disclosure

Marvicap Limited requirements are to establish and maintain a register of all disclosures made to CySEC. There is certain information that this register must capture and our register contains all

of the required information. The register is maintained by the MLRO and is confidential to the MLRO. Records relating to disclosures must be retained for as long as CySEC requires and if we want to destroy these records, the MLRO will be responsible for liaising with CySEC in this regard.

7.5 Money laundering or terrorist financing enquiries

Should you receive any money laundering or terrorist financing enquiries from any party, whether they state that they are entitled to enquire or not, you must pass the enquiry onto the MLRO. In this situation you must be particularly mindful of the offence of "Tipping Off".

7.6 Reporting declined business

A situation may arise in dealing with a potential customer where we decline the business because we feel that there may be an element of criminality involved. In such situations, we are obliged to report the matter to the MLRO even where no transaction has actually taken place. You should note on your report that the business was declined.

7.7 Offences specific to the MLRO

There are some offences specific to the MLRO which are set out below. It is important that all of our staff support the MLRO in his activities and comply with requests for information on a timely basis.

7.7.1 Failure to disclose

The MLRO commits the offence of failure to disclose, separate from the offence described in Section 3, if the following four conditions are satisfied:

1 He knows or suspects or has reasonable grounds for knowing or suspecting that another person is engaged in money laundering; and
2 The basis of the knowledge or suspicion came to him as a result of a disclosure; and
3 The identity of the other person or the location of the laundered property is known or it is believed that the information which the MLRO has will assist; and
4 A disclosure is not made to CySEC.

The MLRO does not commit the offence of failure to disclose if he has a reasonable excuse for not making the disclosure

7.7.2 Consent

The MLRO commits an offence if he gives consent to a prohibited act where none of the following conditions are satisfied and he knows or suspects that the act is a prohibited act:

1 The MLRO has made a disclosure to CySEC and consent has been received; or
2 The MLRO has made a disclosure to CySEC and consent has not been refused within the notice period; or
3 The MLRO has made a disclosure to CySEC, consent was refused during the notice period and the moratorium period has expired.

The MLRO is familiar with the meanings of 'notice period' and 'moratorium period' under the Proceeds of Crime Act.

It is important for you to remember that you should not undertake a transaction on which you have made a suspicious transaction report until you receive consent from the MLRO. To allow funds to be received in, for example, or to make a payment out where you have made a suspicious transaction report and have not received consent, may constitute a prohibited act as referred to above.

7.7.3 Form and manner of disclosures

The MLRO commits an offence if he makes a disclosure to CySEC which is not in the prescribed form. CySEC has a specific form which the MLRO must use for disclosures and the MLRO is aware of the need to use this form.

The MLRO does not commit an offence if he has a reasonable excuse for not using the prescribed form for the disclosure.

7.7.4 Disclosure orders

A disclosure order is an order which requires Marvicap Limited to answer questions, provide information or produce documents in a specified manner at a specified place and time. This will usually be served on the MLRO.

The MLRO will commit an offence if, without reasonable excuse, he fails to comply with a requirement imposed under a disclosure order.

The MLRO will also commit an offence if, in purported compliance with a disclosure order, he provides false or misleading information.

7.7.5 Customer Information Orders

A Customer Information Order is an order which requires Marvicap Limited to provide specific customer information on the person specified in the Order. Such an Order would usually be served on the MLRO.

Marvicap Limited will commit an offence if, without reasonable excuse, it fails to comply with a requirement imposed on it under a Customer Information Order.

Marvicap Limited will also commit an offence if, in purported compliance with a Customer Information Order, it provides false or misleading information.

Section 8 - Record keeping

8.1 Introduction

Record keeping is an essential component of audit trail procedures to ensure that tracing and confiscation of criminal and terrorist funds can be made.

It is essential that our records are sufficient to demonstrate our compliance, particularly if these have to be inspected by CySEC. We must have clear and comprehensive Customer Due Diligence records and transaction records which support the suspicious transactions that we identified and what we did about them.

It is vital, therefore, that you follow the record keeping procedures closely and ensure that records include any meetings, discussions or telephone calls that you have with our clients.

8.2 Identity and Customer Due Diligence records

Our records relating to verification of identity must comprise the original evidence or a copy of it or if we have relied on someone else, for example an Eligible Introducer, information as to where we could get a copy. Section 5 explains the Customer Due diligence information and documentation that we must collect and record.

We must hold these records for five years from the end of the business relationship with our customer or longer if CySEC requires us to.

Where client records come up for destruction, it is part of our policy that the records will be advised to the MLRO and the MLRO will liaise with CySEC, if required, to determine whether the records can be destroyed.

8.3 Transaction records

In addition to identification and verification records, we are required to maintain records of all the transactions that we undertake on behalf of our clients. For each transaction undertaken, the accompanying records must contain:

1) details of the customer or the counterparty and the account details;

2) the nature of the transaction; and

3) details of the transaction.

Where possible, our transaction records should also be able to show:

- The volume of funds flowing through the account / turnover of the client;
- The form in which the funds were paid in or taken out;
- The identity of the person undertaking the transaction;
- The destination of the funds;
- Whether the transaction was a purchase or a win;
- The form and destination of payment made by us to the client; and
- Any large item/exception reports created in the course of transaction monitoring.

It is important that all records pertaining to transactions are filed as soon as possible on the client files within CRM and that any additional information that you obtain from our customers in relation to their transactions are added to these records.

We must hold these records for five years from the completion of the transaction or longer if CySEC requires us to.

8.4 Training Records

Marvicap Limited ensures certain levels of Anti-Money Laundering and Counter-Financing of Terrorism training for all staff which is explained further in Section 9 of this Manual.
We also maintain the following records in respect of the training undertaken as follows:

- The content of the training programmes provided;
- The names of staff who have received the training;
- The date on which the training was delivered; and
- The results of any testing carried out as a result of the Anti-Money Laundering training.

Paul Whelan is responsible for maintaining our anti-money laundering training records and for ensuring that they meet the above requirements.

8.5 Records kept by the MLRO

As referred to in Section 7, the MLRO is required to maintain an enquiries register as well as a disclosures register and a register of internal suspicious transaction reports. These are to record enquiries from CySEC, disclosures to CySEC and reports made by our staff. There are certain fields which these registers have to include and our registers meet these requirements. The registers are maintained by the MLRO and are only available to the MLRO.

8.6 Format and retrieval of records

Marvicap Limited ensures that all of the records outlined above must be capable of retrieval and that:

- Where we keep our records in the form of hard copies, they must be capable of retrieval without undue delay; and

- Where we keep our records electronically, they must be readily accessible and capable of retrieval without undue delay.

We keep our records in hard copy and electronic form and we are satisfied that we are able to retrieve our records without undue delay.

Our disaster recovery plan includes procedures for the retrieval of records and we test our plan on an annual basis.

8.7 Responding to production orders

We must be in a position to retrieve relevant information without undue delay in response to production orders etc. A production order permits CySEC or some other authority to request relevant documents and information. Any such requests for information should be immediately directed to Paul Whelan.

Section 9 – Staff Screening and Training

9.1 Introduction

Marvicap Limited screens new staff members (Directors and employees) and provides training to different categories of staff. This Section of the Manual will explain how we screen new members of staff and also the different forms of anti-money laundering training that we provide.

Marvicap Limited performs due diligence on new directors and all appropriate employees and workers to ensure it is satisfied with Integrity.

Marvicap Limited makes no distinction between different types of director (non-executive directors for example) and expects due diligence to be performed and documented for anybody to whom is assigned a directorship.

Marvicap Limited considers appropriate employees and workers to be those who have access to customers, customer information, company records, systems, hardware and software. In order to meet these requirements, Marvicap Limited will where possible:- obtain and confirm references; confirm employment history and qualifications advised; request details of any regulatory action

taken against the individual (or the absence of such action); request details of any criminal convictions (or absence of such convictions) and verify where possible.

Marvicap Limited documents the steps taken to satisfy these requirements including the information and confirmations obtained.

Marvicap Limited also documents where it has not been possible to obtain such information including reasons why this is the case.

Marvicap Limited will endeavour to make ongoing character checks a part of appropriate employees' employment contracts.

9.2 Staff screening and training policy

Marvicap has a clear and well-articulated policy which ensures that our employees are screened for anti-money laundering purposes and that they are trained in various aspects of the legal and regulatory environment as well as in our own procedures. Our staff screening and training policy has been developed by the MLRO. The information in this Section is in accordance with that policy. The policy will be reviewed on an annual basis by the MLRO and any changes impacting on you will be communicated to you by the MLRO.

The policy extends to temporary and contract staff who may work for us or any outsourced services. The MLRO is responsible for ensuring that all these categories of staff are aware of our anti-money laundering requirements.

9.3 Staff screening

Marvicap Limited maintains and operates procedures which enable us to be satisfied as to the integrity of all new staff. To meet this requirement, the Guidance requires us to do the following in relation to each new staff member:

1) obtain and confirm references;

2) confirm their employment history and the qualifications they say they have;

3) request details of any regulatory action taken against them; and

4) request details of any criminal convictions and verify these where possible.

The MLRO is responsible for undertaking all of the above checks in relation to new members of staff and for retaining the appropriate records. In addition to these checks, we may undertake further open source information searches via the internet.

9.4 Staff training

9.4.1 What must be included in staff training?

It is required to cover:

- The provisions of the anti-money laundering and counter financing of terrorism legislation;
- Their personal obligations under the legislation;
- The internal reporting procedures;
- Their personal liability for failure to report information in accordance with internal procedures;
- Marvicap Limited policies and procedures to prevent money laundering and terrorist financing;
- Marvicap Limited customer identification, record keeping and other procedures;
- The recognition and handling of suspicious transactions; and
- New developments including information on current techniques, methods and trends in money laundering and the financing of terrorism and the EU 6th Anti-Money Laundering directive.

9.4.2 How and when will training be delivered?

All new staff will receive a copy of this Manual/directions to this Manual within their first week and will be required to confirm to the MLRO that they have read and understood it by the end of their first month of employment. All new staff will also receive induction anti-money laundering training. This training is organised by the MLRO. A new member of staff will only be able to become involved in dealing with customers when they have had this training.

On the job training will be delivered to customer facing staff on an ongoing basis. This will include the procedures that we use to conduct a risk assessment of the customer as well as our procedures for Customer Due Diligence.

Refresher training will be delivered on an annual basis. The MLRO maintains the anti-money laundering training records and will be responsible for liaising with all managers to ensure that the training is delivered on a timely basis.

In addition to the above, the MLRO will, from time to time, issue additional information to all staff if there are developments of which staff need to be aware or there has been a change in the legislation or regulation which impacts on our procedures.

Where an employee changes job within the business, consideration will be given as to whether additional anti-money laundering training is required. It is the responsibility of Managers to

discuss whether additional training is required with the MLRO and to record the results in Training Records Register.

Training shall be provided for management and all directors on their responsibilities. This includes all those individuals who act as directors and secretaries of client companies.

The MLRO requires a much more detailed level of training on anti-money laundering and counter financing of terrorism. The MLRO will, therefore, routinely attend external seminars and briefings. Details of these will be recorded in training register.

9.4.3 How is the effectiveness of the training monitored?

The MLRO will monitor the effectiveness of the anti-money laundering training provided. We do this by:

- Requiring all staff to undertake a test following the induction and refresher anti-money laundering training, the results of which are retained by the MLRO;
- Monitoring compliance with our anti-money laundering procedures by annual reviewing compliance and ensuring that any remedial action is taken and is supported by further training, where necessary.
- Monitoring the pattern and quality of internal suspicious transaction reports and providing further training, where necessary.
- Assessing any court orders, we receive to determine whether suspicions were recognised and disclosed.