# ANTI-MONEY LAUNDERING AND COUNTERING TERRORIST FINANCING MANUAL

Approved by the Board:
June 2018 (Last review June 2021)
CONTENTS

DOMINION
CAPITAL STRATEGIES

# CONTENT

## GLOSSARY OF TERMS

| | |
|---|---|
| ABC | Anti-bribery and corruption |
| All Crimes Law | The Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999 as amended |
| AML/CFT | Anti-money laundering and countering terrorist financing |
| Al-Qaida Ordinance | The Al-Qaida (Restrictive Measure) (Guernsey) Ordinance, 2013 |
| CDD | Customer Due Diligence |
| CIS | Collective investment schemes |
| Compliance Support | Cannon Asset Management Limited |
| CTC | Certified true copy |
| DCSL and Company | Dominion Capital Strategies Limited |
| DL | The Disclosure (Bailiwick of Guernsey) Law, 2007, as amended |
| DTL | The Drug Trafficking (Bailiwick of Guernsey) Law, 2000 as amended |
| EDD | Enhanced Due Diligence |
| EU | European Union |
| FATF | Financial Action Task Force |
| FIS | Financial Intelligence Service |
| FIU | Financial Investigation Unit |
| FSB | Financial Services Business |
| GBA | Guernsey Border Agency |
| GFSC | Guernsey Financial Services Commission |
| Guernsey Corruption Law | The Prevention of Corruption (Bailiwick) of Guernsey Law, 2003 as amended |
| Handbook | The Handbook for Financial Services Businesses on Countering Financial Crime and Terrorist Financing |
| IMF | International Monetary Fund |
| Introducers | Those financial advisers or other introducers of potential investors into DCSL |
| MLRO | Money Laundering Reporting Officer |

| | |
|---|---|
| NO | Nominated Officer |
| OFAC | Offices of Foreign Assets Control |
| PEPs | Politically Exposed Persons |
| Portal | The digital investment portal, pursuant to which clients access DCSL |
| T&CL | The Terrorism and Crime (Bailiwick of Guernsey) Law, 2002 as amended |
| Terrorism Law | The Terrorist Asset-Freezing (Bailiwick of Guernsey) Law, 2011 as amended |
| The Act | The Bribery Act 2010 |
| UN | United Nations |
| 2007 Regulations | The Criminal Justice (Proceeds of Crime) (Financial Services Businesses) (Bailiwick of Guernsey) Regulations, 2007 as amended |

## 1. ANTI-MONEY LAUNDERING AND COUNTERING TERRORIST FINANCING

### 1.1 POLICY

DCSL will not be involved with any entity that is involved with Money Laundering or Financing of Terrorism and staff and Introducers should do everything possible to prevent such involvement. The fundamental aim is the protection of the integrity of DCSL, Guernsey, the wider Dominion Group and its staff.

AML/CFT has been the subject of legislation throughout the world in recent years. In particular, countries which are members of the Financial Action Task Force have committed themselves to implementing a set of recommendations which are more wide ranging than other standards and are generally accepted as the highest applicable standard, against which DCSL has benchmarked itself as best practice.

### 1.2 WHAT IS MONEY-LAUNDERING?

The expression "money laundering" covers all activities that conceal and disconnect the origins of criminal proceeds from the criminal, so that they appear to have originated from a legitimate source.
Two main indicators of Money Laundering are:

- An arrangement or transaction between two or more parties involving property which has been acquired criminally or by the proceeds of crime.

- Suspicion or knowledge that property has been acquired criminally or by the proceeds of crime.

The intended purpose of the transaction is:

- to conceal the true ownership and origin of criminal proceeds;

- to maintain control over them; and

- to change their form.

Individual transactions may only be a small part of a bigger picture.

### 1.3 WHAT IS FINANCING OF TERRORISM

For terrorists, the acquisition of funds is not an end in itself but a means of committing a terrorist attack. With terrorist financing, it does not matter whether the transmitted funds come from a legal or illegal source as terrorist financing frequently involves funds that, prior to being remitted, do not necessarily derive from criminal activity.

Tracking terrorist financial transactions arising from legitimate sources is more difficult than following the money trails of the proceeds of crime because of the relatively small amounts of funds required for terrorist actions and the range of legitimate sources and uses of funds. Terrorist attacks are in many cases comparatively inexpensive, and their financing is often overshadowed by the larger financial resources allocated for the group's political and social activities, making it more difficult to uncover the illicit connections.

Identifying and disrupting the mechanisms through which terrorism is financed are key elements in the overall

efforts to combat terrorism. As well as reducing the financial flows to terrorists and disrupting their activities, action to counter terrorist financing can provide vital information on terrorists and their networks, which in turn improves law enforcement agencies' ability to undertake successful investigations.

The Company can assist governments and their agencies in the fight against terrorism through prevention, detection and information sharing. The Company seeks to prevent terrorist organizations from accessing the funds that they administer, assist governments in their efforts to detect suspected terrorist financing and promptly respond to governmental enquiries.

Recognising the difficulties inherent in identifying financial transactions linked to the financing of terrorism (many of which appear routine in relation to information known at the time) DCSL has implemented monitoring procedures for identifying and reporting unusual or suspicious transactions which may assist governmental agencies by linking seemingly unrelated activity to the financing of terrorism.
DCSL is committed to:

- The proper verification of the identity of clients.
- Exercising increased monitoring of clients identified as high risk.
- Monitoring for unusual transactions
- Ongoing monitoring of clients against lists generated by competent authorities of known or suspected terrorists or terrorist organisations.

This procedure outlines DCSL's policy and procedures that guard against:

- DCSL being used for money laundering or financing terrorism.
- The committing of an offence under the relevant laws by DCSL itself or its employees.

### 1.4 GUERNSEY'S ANTI-MONEY LAUNDERING AUTHORITIES

#### 1.4.1 Guernsey Financial Services Commission

The GFSC is DCSL's regulator. It was established by the Financial Services Commission (Bailiwick of Guernsey) Law, 1987 and is a body corporate independent of government. It is funded by the fees it charges the firms it regulates. The Division at the GFSC responsible for regulating DCSL is the Fiduciary Supervision Policy and Innovations Division. Compliance will review the GFSC's website regularly (www.gfsc.gg) in order to keep abreast of regulatory changes taking place in Guernsey and will inform the Directors and Staff accordingly.

#### 1.4.2 The Financial Investigation Unit

The FIU is part of the GBA and is responsible for the investigation of all Guernsey financial crime other than domestic fraud. The FIU is divided into three sections:

- Financial Intelligence Service

This is a team of police and GBA staff who receive suspicious transaction/activity reports from financial services businesses, lawyers, accountants and estate agents. They provide relevant financial intelligence in order to assist Guernsey and international investigations;

- Civil Forfeiture Team

  This Team deals with the proceeds of unlawful conduct which have been deposited in Guernsey bank accounts or held in cash locally. It seeks to confiscate the criminal's proceeds of crime under the civil law burden of proof where a criminal case could not be brought to court; and
- Financial Crime Team

  This Team investigates suspected money laundering offences that may have been committed in the Bailiwick, criminal confiscation and other financial and economic crime with a view to prosecution.

**1.5 LAWS AND REGULATIONS**

The "relevant laws" relating to money laundering are:

**1.5.1 The Drug Trafficking (Bailiwick of Guernsey) Law, 2000 as amended**

The DTL came into force on the 1 January 2000. It contains provisions for: The creation of six offences relating to money laundering associated with Drug Trafficking (section 57 - 62):

- Concealing or transferring proceeds of Drug Trafficking.
- Assisting another person to retain the benefit of Drug Trafficking.
- Acquisition, Possession or Use of Proceeds of Drug Trafficking.

A person found guilty of the above offences is liable to a maximum of 14 years' imprisonment.

- Failure to Disclose Knowledge or Suspicion of Money Laundering.
- Tipping Off.
- Prejudicing an Investigation.

A person found guilty of the above offences is liable to a maximum of 5 years' imprisonment.

**1.5.2 The Terrorism and Crime (Bailiwick of Guernsey) Law, 2002 as amended**

The T&CL came into force on 19 July 2002. Under the provisions of the T&CL, if a person believes or suspects another person has raised funds for terrorists, possessed money for use in terrorism, become involved in making funding arrangements or the laundering of money connected with terrorism and the belief or suspicion arises during the course of a trade, profession, business or employment, the relevant information must be passed to the law enforcement authorities. Failure to do so is an offence.

The requirement of financial services businesses to report suspicion concerning offences connected with the financing of terrorism is extended to circumstances where the person in the financial services business has reasonable grounds for knowing or suspecting that a person has committed an offence.
The T&CL also contains a money laundering provision. A person commits an offence if he enters into or becomes concerned in an arrangement which facilitates the retention or control by or on behalf of another person of terrorist property:

- by concealment;

- by removal from the jurisdiction;
- by transfer to nominees; or
- in any other way.

It is a defence for a person charged with a money laundering offence under the T&CL to prove that he did not know and had no reasonable cause to suspect that the arrangement related to terrorist property.

The T&CL also contains a number of other offences, which include those relating to the financing of terrorism (sections 8 to 10); money laundering (section 11) and tipping off (section 40).

### 1.5.3 The Disclosure (Bailiwick of Guernsey) Law, 2007 as amended

This Law places an obligation to disclose to the authorities any suspicion concerning money laundering.

Section 1 of the DL states that a person commits an offence if:

a) he/she knows or suspects or has reasonable grounds for knowing or suspecting that another person is engaged in money laundering; and
b) the information (or other matter) on which his or her knowledge/suspicion is based (or which gives reasonable grounds for such knowledge or suspicion) came to him/her in the course of the business of a financial services business; and
c) he/she does not make a disclosure as soon as is practicable after the information (or other matter) came to him/her.

Therefore, the DL introduces a positive obligation to disclose suspicions. This is very important as a person would potentially be guilty of an offence not only if they fail to report a knowledge or suspicion, but also if they fail to report where they have "reasonable grounds for knowing or suspecting" that another person is engaged in money laundering. This test of knowledge or suspicion in the DL is what is known as an "objective test".

This means that if a reasonable man or woman employed by a financial services business (with their knowledge and experience) would "know or suspect" money laundering might be taking place, that will be enough for them to be found guilty of an offence if they do not report it to the MLRO.

### 1.5.4 The Terrorist Asset Freezing (Bailiwick of Guernsey) Law, 2011 as amended

UN Security Council Resolution 1373 and Council Regulation (EC) No. 2580/2001 imposes restrictive measures directed against certain persons and entities with a view to combatting terrorism.

It is a criminal offence under the Terrorism Law for DCSL to fail to disclose to the Policy Council its knowledge or suspicion that an investor is a designated person or has committed an offence as set out in the Terrorism Law. This is additional requirement to DCSL' reporting obligations under the DL and the T&CL Laws.

### 1.5.5 The Al-Qaida (Restrictive Measures) (Guernsey) Ordinance, 2013 (the Al-Qaida Ordinance)

The Al-Qaida Ordinance replaces the Al-Qaida and Taliban (Freezing of Funds)

(Guernsey) Ordinance, 2011, which has now been repealed. This new Al-Qaida Ordinance takes into account recent amendments to EU measures. It also introduces reporting obligations to the Policy Council in Guernsey.

The Policy Council must be notified as soon as practicable if DCSL knows or has reasonable cause to suspect, that a client:

- is a designated person;
- has breached any of the prohibitions in the Ordinance; and
- the information or other matter on which the knowledge or reasonable cause of suspicion is based came to DCSL in the course of carrying on it business. There is also an obligation to state the nature and amount of any funds/economic resources held by DCSL for the client at the time when DCSL first had the necessary knowledge or suspicion. It should be noted that failure to comply with this reporting obligation is a criminal offence punishable with up to 12 months' imprisonment or a fine up to £5,000.

This reporting obligation is in addition to the existing obligation to report suspicion of money laundering or terrorist financing to the Financial Intelligence Service under the Disclosure (Bailiwick of Guernsey) Law 2007 as amended and/or the Terrorism and Crime (Bailiwick of Guernsey) Law 2002 as amended. DCSL needs to be aware of these measures and must continue to ensure thatey it does not maintain any accounts or otherwise hold any funds or economic resources for the entities and individuals named in the HM Treasury consolidated list.

### 1.5.6 The Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999 as amended

The All Crimes Law, which came into force on 1 January 2000, extends the application of the anti-money laundering laws to include all criminal conduct which:

- constitutes a criminal offence under the Laws of the Bailiwick which may be tried on indictment or;
- would constitute such an offence if it were to take place in the Bailiwick.

There are five principle offences:

- concealing or transferring the proceeds of criminal conduct;
- assisting another to retain the benefit of criminal conduct;
- acquiring, processing or using the proceeds of criminal conduct;
- tipping off - "disclosure of any information or any other matter which is likely to prejudice any investigation which might be conducted following the disclosure"; and
- prejudicing an investigation.

### 1.5.7 The Criminal Justice (Proceeds of Crime) (Financial Services Businesses) (Bailiwick of Guernsey) Regulations, 2007 as amended

The 2007 Regulations require all FSBs to have and maintain AML/CFT Policies, procedures and controls.

The Handbook has been issued by the GFSC and is divided into two levels, Commission Rules and Guidance. It sets out how the GFSC requires FSBs to comply and meet the Regulations and Rules. In addition, it also sets out the GFSC's enforcement policy under the regulatory laws for any contravention of the Commission Rules or Regulations.

An FSB may adopt other appropriate and effective measures to those set out in Guidance, including policies, procedures and controls established by the group Head Office of the financial services business, so long as it can demonstrate that such measures also achieve compliance with the Regulations and the Commission Rules.

DCSL's procedures will evidence compliance with the GFSC's Handbook for Financial Services Businesses on Countering Financial Crime and Terrorist Financing (as amended).

The 2007 Regulations and the Handbook require DCSL to adopt a risk based approach to its policies, procedures and controls in relation to AML/CFT taking into account its clients and the services they are provided with both to the extent of its CDD measures and for the ongoing monitoring of business relationships. High risk clients or Products or Services and transactions are subject to a higher level and frequency of monitoring.

In compliance with the above requirements, DCSL will risk profile both its Clients and Services and the procedures for this are detailed later in this section under the heading Risk Profiling.

### 1.5.8 The Transfer of Funds (Guernsey) Ordinance, 2007

This Ordinance applies to the transfers of funds in any currency which are sent or received by a Guernsey payment service provider. A "payment service provider" is a person (normally a bank) whose business is the provision of transfer of funds services. The Ordinance – a prevention of terrorist financing requirement – requires that transfers of funds must be accompanied by complete information on the payer, generally their name, address and account number.

However, the address can be replaced by a date and place of birth, his or her client identification number (if he/she has one) or national identity number and, where the payer does not have an account number, the payment service provider needs to insert a unique identifier which allows the transaction in question to be traced back to the payer.

The law contains certain requirements placed on payment service providers, for example relating to verification of payers' identities. Staff should be aware that payment service providers might need to request detailed information on any of DCSL's clients seeking to make transfers. In light of the requirements of this Ordinance, full cooperation should be given to payment service providers.
There are equivalent Alderney and Sark laws.

## 1.6 GENERAL PROCEDURES

1.6.1 DCSL has adopted written procedures to comply with the requirements of the All Crime Law, the 2007 Regulations and the Handbook.

1.6.2 DCSL will not accept a new client or Introducer prior to checking the client against recognised systems and web searches. However, this is not an exhaustive description of the verification process, as each client will be reviewed oin a case-by-case basis. DCSL will endeavour to meet as many new clients as reasonably possible on a face-to-face basis during the earlier stages of the relationship.

1.6.3 The DCSL Board will ensure that the GFSC is advised of any material failure to comply with the 2007 Regulations and the Rules in the Handbook and any serious and/or material failure of DCSL's policies, procedures and controls.

### 1.7 SPECIFIC PROCEDURES

All staff are responsible individually pursuant to the AML/CFT Laws to comply with the obligations set out in this document. Compliance with these procedures will discharge those obligations. All staff must comply with the following:
· Monitoring business relationships (including review of identification data on a risk profiled basis)

· Monitoring transactions for unusual/suspicious transactions

· Reporting of suspicious transactions

· Verification procedures for new clients

· Verification procedure for client dealing

· Record keeping

· Training (attending and completing)

· UN, EU and other sanctions

## 2. CORPORATE GOVERNANCE

### 2.1 BOARD RESPONSIBILITY

The 2007 Regulations and the Handbook place great emphasis on the Board collectively taking effective responsibility for compliance with the Regulations and the Handbook. The Handbook also places responsibility on the Board for establishing and maintaining an effective policy for reviewing its compliance with the 2007 Regulations and the Handbook. Such a review is to be carried out at least annually.

In accordance with the requirements of the Handbook, the Board will:

- ensure that the compliance review policy includes a requirement for sample testing of the effectiveness and adequacy of the policies, procedures and controls;
- consider annually whether it would be appropriate to maintain a separate internal audit function to assess the adequacy and effectiveness of the area of compliance;
- ensure that when a review of compliance is discussed by the Board the necessary action is taken to remedy any identified deficiencies;

- provide adequate resources either from within DCSL or externally to ensure that the AML/CFT policies, procedures and controls are subject to regular monitoring and testing;

- provide adequate resources to enable the MLRO to perform their duties; and • take appropriate measures to keep abreast of and guard against the use of technological developments and new methodologies in money laundering and terrorist financing schemes.

The Board must advise the GFSC of any material failure to comply with the 2007

Regulations or the Handbook Rules or any serious breaches of DCSL's AML/CFT

Policies and Procedures.

**2.2 MLRO RESPONSIBILITIES**

DCSL's MLRO is Kevin Wakeham.
The MLRO appointed must:

- be a natural person;
- be employed by the business;
- be of at least management level;
- be resident in Guernsey;
- be the main point of contact of the FIS in the handling of disclosures;
- have sufficient resources to perform his duties;
- be available on a day to day basis;
- manage the risk of tipping off;
- receive full cooperation from all staff;
- report directly to the Board
- have regular contact with the Board to ensure that the Board is able to satisfy itself that all statutory obligations and provisions in the Handbook are met and that the business is taking sufficiently robust measures to protect it against the potential of being used for money laundering and terrorist financing; and be fully aware of both his obligations and those of DCSL's under the Regulations, the relevant enactments and the Handbook.

The NO must be management level or above and be available in the absence of the MLRO.

**2.3 MLRO POLICY**

Sufficient resources will be made available to the MLRO to enable them to carry out their duties and responsibilities. The MLRO will have access to all of DCSL's files and should receive full cooperation from all staff. The MLRO has full and free access to the Board at all times.

**3. RISK BASED APPROACH**

**3.1 POLICY**

The Handbook was issued on 15 December 2007 and is amended from time to time. In conjunction with the 2007 Regulations which also came into force on the same date, they require DCSL to adopt a risk based approach to its policies, procedures and controls in relation to AML/CFT, taking into account its clients and its products. DCSL is also required to carry out a suitable and sufficient business risk assessment in order to identify any AML/CFT risks and then must set out how it will manage and mitigate these risks. The risks of DCSL being used for bribery and corruption should also be considered in the same way and please see section 5:15 in this regard.

The Handbook and 2007 Regulations stipulate that DCSL should take risk into account when determining the extent of its CDD measures. The 2007 Regulations and The Handbook allow DCSL to apply reduced or simplified measures for low risk clients. Conversely, they require DCSL to carry out EDD for high risk categories of clients and transactions.

The 2007 Regulations and The Handbook also contain provisions for the ongoing monitoring of business relationships – high risk clients and transactions are subject to a higher level and frequency of monitoring.

In compliance with the above requirements, DCSL will risk profile both its clients and its risk profiling policy to ensure it is in accordance with the 2007 Regulations and the Handbook.

### 3.2 BUSINESS RISK ASSESSMENT

DCSL's Board has adopted an AML/CFT Business Risk Assessment as required under Regulation 3 of the 2007 Regulations. This is documented and specific to its business. This includes an assessment of the bribery and corruption risks to DCSL's business.

At least once a year, or when DCSL's business risk profile changes significantly, the Board will carry out a review of this Business Risk Assessment. This may be delegated to the MLRO, the Nominated Officer and any external or internal resources deemed appropriate by the Board.

The revised draft Business Risk Assessment will be based on the review, drawing on findings from the monitoring programme, the reviewers and the Board's ongoing knowledge of DCSL's client base. The Board will make the necessary changes to the draft Business Risk Assessment and approve it. They will then ensure that DCSL's policies, procedures and controls on AML/CFT are appropriate and effective in light of the revised Business Risk Assessment.

### 3.3 RELATIONSHIP RISK ASSESSMENT

For each new client or Introducer relationship, DCSL will complete a relationship risk assessment before establishing the business relationship. This will ensure that all relevant risk factors have been considered prior to determining a risk rating classification of the potential client and whether or not to accept them. The risk levels set are high, standard and low.

Risk rating is a process by which consideration is given to the identity of the client, beneficial owners and underlying principals and their nationality, domicile and residency; associated geographic areas, the purpose and intended nature of the business relationship; and the type, volume and value of activity that can be expected within the business relationship and the product/services being utilised and the delivery channel that will be used to provide such services. DCSL will also assess the client's risk in the light of DCSL's own Business Risk Assessment prior to the establishment of the business relationship to ensure that the risks are fully understood, managed and mitigated accordingly.

The risk rating will determine how the business is conducted and the frequency with which a review of the entity and their affairs is undertaken. The level of CDD verification at the point of acceptance of the client is dependent upon the risk profile.
All Risk Ratings applied must be approved by DCSL. In the initial phase of operation of the Company from commencing operations external compliance will review all Risk Ratings and take on forms (physical or digital) for accuracy and completeness.

Where one or more aspects of the business relationship or occasional transaction indicates a high risk of money laundering or terrorist financing but DCSL does not assess the overall risk as high because of strong and compelling mitigating factors, DCSL must identify the mitigating factors and, along with the reasons for the decision document them. After this is concluded, the risk rating may be downgraded to standard. However, DCSL must ensure that any proposed or existing business relationship or any proposed occasional transaction which either has characteristics identified in Regulations 5(1) (a) to (c) or is connected to any of the countries listed in part A or Part C of Instructions issued by the Commission is designated as high risk.

Should any risk factors change then the Risk Rating applied should be reassessed and amended and approved as applicable. Note that if the risk rating is revised upwards, it is likely that further CDD will be required.

**3.4 CLIENT - HIGH RISK INDICATORS**

In accordance with Rule 58 of the Handbook and Regulation 5 of the 2007

Regulations, if the business relationship indicates one of the following, the Risk Rating MUST BE High Risk:

- Involvement with a Politically Exposed Persons (refer to separate section for full details);

- where the business relationship is in respect of the provision of services which themselves amount to financial services business or facilitate the carrying on of such business;
- where the client is established or situated in a country or territory that does not apply or insufficiently applies the Financial Action Task Force Recommendations on Money Laundering (refer to Country list for full details);
- Clients who DCSL considers to bethe high risk following the release of any notices, instructions or warnings issued from time to time by the GFSC, (specifically Parts A & C of the GFSC Instructions). In terms of other high risk indicators, should one or more of the following indicators appear when assessing a client's Risk then a High Risk rating should also be applied to the client:
- overly complex structures, which can make it easier to conceal underlying beneficial owners and beneficiaries;
- structures with no apparent legitimate or economic rationale for establishment when similar products are available in his home country;
- clients who request the use of general powers of attorney in a manner which dilutes the control of a company's directors;
- relationships where the source of wealth/funds cannot easily be verified;

- clients based in, or conducting business in or through, a country or territory with known higher levels of bribery and corruption, or organised crime, or involved in illegal drug production/processing/distribution, or associated with terrorism; • involvement of introducers from a country or territory which does not have sufficient AML/CFT infrastructure;
- request for safe custody arrangements;

- request for significant and or frequent cash transactions, high value balances or investments, which are disproportionately large to the particular client, product or service;
- Commercially Exposed Persons (refer to separate section for full details); • clients or structures which are associated with a specific industry activity which carries a higher exposure to the possibility of bribery and corruption (such as in natural resource extraction, infrastructure construction or the defence industry);
- where the client requests undue levels of secrecy (e.g. hold mail facilities, bearer instruments);

- Clients who wish to operate active trading, re-invoicing or offshore employment companies. However, if there are strong and compelling mitigating factors, DCSL must identify these mitigating factors and, along with the reasons for the decision document them. Thereafter the Directors can determine to lower the risk rating from high risk to standard risk if considered appropriate. Note: This down grading to Standard risk does

not apply to any business relationships with the characteristics set out in Rule 58 of the Handbook or Regulation 5(1)(b) or (c), as above.

### 3.5 CLIENT – LOW RISK INDICATORS

The following may be considered to be low risk indicators when assessing a

client's risk rating:

- clients whose funds are part of a pooled client money account held in the name of an Appendix C business (see the definition in Appendix C to the Handbook);
- clients who are actively employed with a regular source of income which is consistent with the employment being undertaken;
- clients who are locally resident retail clients who have a business relationship which is understood by the financial services business; and
- clients represented by those whose appointment is subject to court approval or ratification (such as executors).

### 3.6 COUNTRY RISK

As well as responding to the Business from Sensitive Sources Notices and other

Instructions from the GFSC, Compliance Support will review the GFSC website regularly for AML/CFT information and other websites as appropriate.

Regardless of whether a country has "equivalence status", DCSL will need to maintain an appropriate degree of ongoing vigilance concerning money laundering and terrorist financing risks and to take into account information that is reasonably available to them about the standards of AML/CFT systems and controls that operate in the country with which any of their clients are associated. AML/CFT risk will vary between countries. To help DCSL assess the degree of country risk, information on the most recent international country assessments and on perceived country risk is reviewed by Compliance Support from the appropriate sources.

Countries identified by GFSC within the Instruction Notices are designated with an asterix (*) cannot have the risk mitigated and must remain High. Changes to the risk rating of countries will be monitored by and notified by Compliance
Support.

### 3.7 POLITICALY EXPOSED PERSONS

PEPs are defined as persons who are or have at any time been entrusted with a prominent public function in a country or territory outside of the Bailiwick. The list below shows examples but should not be considered exhaustive of such persons holding prominent public positions (both current and former positions held):

- Heads of State or of Government
- Senior Politicians and other important officials of political parties
- Senior Government, judicial, military or officials
- Senior Executives of State-Owned enterprises

The definition of a PEP also includes:

- an immediate family member of such a person including, without limitation, a spouse, partner, parent, child, sibling, parent-in-law or grandchild of such a person and partner means a person who is considered by the law of the country or territory in which the relevant public function is held as being equivalent to a spouse or;
- a close associate of such a person, including, without limitation

  - a person who is widely known to maintain a close business relationship with such a person, or
  - a person who is in a position to conduct substantial financial transactions on behalf of such a person.

The definition is not intended to cover middle ranking or more junior individuals in the foregoing categories but DCSL should also be cautious when asked to act for such individuals.

In Guernsey legislation, once an individual has been classified as a PEP he/she will always remain a PEP. Before entering into a business relationship with a PEP, ensure that sign off has been completed by Compliance Support in addition to a Director. Compliance Support will maintain the PEP register and conduct enhanced monitoring.

### 3.8 PRODUCT RISK INDICATORS

In accordance with the Handbook, all products and services provided by DCSL are risk rated by the Board. Such risk ratings are reviewed regularly.

In accordance with the Handbook, the following are considered to be low risk indicators when assessing the products risk rating:
• products where the provider does not permit third party investment or repayment and the ability to make or receive payments to or from third parties is restricted.

The following are guideline risk ratings. Individual circumstances may require an alternative assessment. Products and Services offered will vary from time to time and where uncertainty exist the risk profiling should be referred to a Director.

#### 3.8.1 Trusts

DCSL's main purpose is to act as trustee for clients, in order to facilitate their investment into Dominion Capital Strategies Fund PCC Limited. The trust formed between DCSL and the client is a discretionary trust, settled at the time of investment by way of a declaration of trust.

Discretionary Trusts, due to their nature and the potential investment risk could, in certain circumstances, be considered as posing a higher risk to DCSL and therefore particular attention should be given to the potential frequency of transactions and investment structure before applying the risk rating.

However, in general, the trusts created by DCSL are simple in their structure, and expose DCSL to a lower level of risk than traditional discretionary trusts. However, the risk rating of a product is only one of several factors that must be considered within the overall business relationship. The overall risk rating rationale must be documented

## 4. CLIENT ACCEPTANCE AND CUSTOMER DUE DILIGENCE

### 4.1 POLICY

DCSL is obligated to identity and verify the identity of any client, beneficial owner or underlying principal of any structure administered in order to establish and be satisfied that:

- the person exists; and
- the client, beneficial owner or underlying principal is that person, by verifying from the identification documentation satisfactory confirmatory evidence of appropriate components of their identity.

### 4.2 ESTABLISHING A BUSINESS RELATIONSHIP

The Directors consider that a business relationship is established at the point when DCSL's Terms and Conditions and Client Application forms have been accepted and countersigned by the Directors on the Portal.

However, should DCSL during any preliminary discussions, have any reasonable grounds for knowing or suspecting that the proposed client was involved in money laundering or terrorist financing as defined by the 2007 Regulations then they would fulfil their obligations by making a report to the MLRO.
Prior to establishing a business relationship DCSL will need to determine whether the client is an Individual or Legal Body and then must determine the Risk Rating to be applied to the Client. This will then enable DCSL to determine what level of CDD information is required.

Following any face-to-face meetings with a prospective client, a file note should be made by the Introducer with any relevant information and/or action points and be signed by the person attending the meeting. Any other relevant documentation obtained at the meeting should also be attached. The file note should form part of the relationship risk profiling form.

At this point, an account opening process may start on the Portal and Client Due Diligence information uploaded appropriately.

In accordance with the Handbook all clients will automatically default to

Standard Risk, until they are reviewed and determined whether they meet with the requirements of Low or High Risk Factors. In cases where the client has been assessed as High Risk, EDD should be carried out in accordance with this manual.

The examples set out over the next few pages are the standards for the Client Due Diligence DCSL should obtain when entering into a new relationship with a Client.

### 4.3 UNACCEPTABLE BUSINESS

It is DCSL policy to NOT enter into a business relationship where the following are applicable:

- knowledge or suspicion of money laundering or terrorist financing or any other crime;
- where DCSL is requested to settle a trust for an illegitimate purpose;
- where structures are requested and despite efforts to do so we cannot identify apparent legitimate economic or other rationale for the structure;
- where the proposed relationship is structured such that the audit trail has been deliberately broken and/or unnecessarily layered;

- where DCSL are requested to establish arrangements which have the apparent objective of fiscal evasion;
- where despite efforts to resolve there is a lack of clarity about beneficial ownership or interests, or DCSL experiences difficulties in verifying identity of persons with ownership or control; or
- where a proposed client is unwilling to provide DCSL with the degree of information and control which it needs to fulfil its duties.

**4.4 STANDARD RISK CDD - INDIVIDUALS**

Identification and verification of an individual is a two-part process. The individual is required to first identify themselves to DCSL by supplying a range of personal information. The second part is verification.

**4.4.1 Identification** - In accordance with the Handbook Rule 86, DCSL is required to obtain the following information:

- legal name, any former names (such as maiden) and any other names used;

- principal residential address;

- date and place of birth;

- nationality (dual nationality where held);

- occupation, public position (where appropriate name of employer); and - an official personal identification number or unique identifier from an unexpired official document (for example, passport, identification card, residence permit, social security records, driving licence) that bears a photograph of the client. In order to comply with Rule 86, DCSL will obtain a duly completed and signed Client Acceptance Form (via the Portal).

**4.4.2 Verification** – In accordance with the Handbook Rule 87 DCSL must verify:

- legal name;

- address;

- date and place of birth; and

- nationality (nationalities, where applicable) and official personal identification number

In order to comply with Rule 87, DCSL will accept one of the following for the purpose of verifying legal name, date and place of birth, nationality and personal identification number.

Duly CTC of the following:

- current valid passport(s) (providing photographic evidence of identity); - current national identity card (providing photographic evidence of identity); or - Armed Forces identity card.

The above is not a conclusive list; in particular countries there may be other documents of equivalent nature which may provide satisfactory evidence of
identity.

In accordance with the Handbook guidance contained in paragraph 90, DCSL will accept one of the following in order to establish confirmation of the individual's principal residential address:

- bank/credit card statements or utility bills (no more than 3 months old) are acceptable. Mobile phone bills are not acceptable;
- correspondence from an independent source e.g. central or local Government department or Agency;
- commercial or electronic databases;

- Letter of introduction from an Appendix C (as defined in the Handbook) financial services business (who confirms that they have an existing business relationship with the client and confirms residential address);
- Written communication from Appendix C (as defined in the Handbook) financial services business in connection with a product or service purchased by the client;
- personal visit to the residential address; or

- an electoral roll.

**4.4.3 Verification of residential address of overseas residents**

Where overseas residents encounter difficulties in providing address verification e.g.:

- residents in countries without postal deliveries;

- no street addresses; or - Post Office Boxes, a letter issued by Director or Officer of a reputable overseas employer who confirms residence or provides detailed directions to locate residence can be accepted as a form of verification of their residence, where applicable, for example a pension scheme:

DCSL should undertake to review and if possible verify the employer by appropriate recognised tools such as C6 and internet searches.

All key documents (or parts thereof) not in English must be translated into English.

**4.5 STANDARD RISK CDD - COMPANIES AND OTHER LEGAL BODIES**

Identification and verification requirements in respect of clients who are not individuals are different from those for individuals. Although a client who is not an individual has a legal status which can be verified, each client also involves a number of individuals. In accordance with the Handbook Rule 109, DCSL MUST identify and verify these individuals which include:

- beneficial owners (or equivalent);

- directors (or equivalent);

- underlying principals, who have power to direct movement of client's funds or assets.

In accordance with the Handbook Rule 110, certain information must be obtained as a minimum requirement. Having assessed the money laundering and terrorist financing risk of the particular client/product/service combination DCSL must consider how the identity of the client and of specific individuals should be verified, and what additional information in respect of the entity must be obtained.

**4.5.1 Legal Bodies**

Legal body refers to Corporate Structures (e.g. Companies - Private, Public Limited Companies), partnerships, associations or other bodies which are not natural or legal arrangements. (Trusts and foundation relationships are dealt with separately.)

In accordance with the Handbook Rule 113, DCSL MUST identify and verify the following:

- name, official identification number, date and country or territory of incorporation (if applicable);
- Registered Office address and principal place of business (if different);

- individuals ultimately holding 25% or more interest in the capital or net assets of the legal body
- Individuals – beneficial owners, underlying principals, directors, authorised signatories or equivalent with ultimate effective control over the capital or assets of the legal body
- Legal status of legal body.

Companies that are regulated firms, quoted on a regulated market or are GFSC regulated collective investment schemes – see low risk below.

DCSL will accept one or more of the following to identify and verify the entities legal status and the controlling parties:

- certificate of incorporation & certificate of name change (if applicable);

- company registry search (if applicable) including confirmation that the company has not been and is not in the process of being, dissolved, struck off, wound up to terminated;

- latest audited financial statements;

- Memorandum and Articles of Association;

- Directors' Register including full names and permanent residential address; • Shareholders' Register including full names and permanent residential addresses of controlling shareholders (natural persons) holding more than 25% of the issued share capital;
- independent information sources, including electronic sources, for example business information services;
- copy of the Board Resolution, authorizing the opening of the account and recording account signatories; or
- personal visit to the principal place of business.

Due Diligence is required on any controlling party holding more than 25% in accordance with the requirements of this Manual.

All copy documentation provided must be certified by an acceptable officer of the Company or a suitable certifier.

If any of the above documentation is obtained directly from Companies House (or equivalent) by a member of Compliance Support, then this should be evidenced accordingly.

All key documents (or parts thereof) must be translated into English.

Any client where the legal body, or any beneficial owner or underlying principal connected with the legal body, presents a high risk, DCSL must consider whether additional verification checks are necessary. See section 5 of this Manual.

#### 4.5.2 Control of Legal Bodies that are not companies

In accordance with Paragraph 118 of the Handbook, a 25% or more interest in the capital or net assets of a legal structure, partnership, association, club, society, charity, church body, institute, mutual and friendly society, or cooperative and provident society is deemed as having effective control/ownership.

Individuals who have ultimate effective control or ownership will often include:

- Partners (Partnerships)
- Members of the governing body or committee (associations, clubs etc.)
- Executives.
- Governing Council/supervisors (foundations)

Due Diligence should be performed accordingly upon any such persons in accordance with the relevant section of this Manual.

It should be noted that even though DCSL adopts and follows The Handbook, some banks deem 10% as effective control and require verification on shareholders, therefore care should be taken to ensure that the correct information is requested.

### 4.6 STANDARD RISK CDD – TRUSTS

#### 4.6.1 DCSL acting as Trustee to a Trust

When establishing a trust, for which DCSL will act as trustee, DCSL must accordance with the Handbook Rule 134, identify and verify the identity each of the following:

- settlor(s) (if applicable); and
- any beneficiary with a vested interest or any person who is or any person who is the object of a power.

Before commencement of a business relationship, DCSL must determine

whether any persons listed above within the relationship are to be classified High Risk. If the answer is "Yes" enhanced due diligence requirements will need to be undertaken in accordance with section 5 of the Manual and Chapter 5 of the Handbook.

Beneficiaries - In accordance with the Handbook Rule 135 verification of the identity of beneficiaries with a vested interest or any person who is the object of a power must be undertaken prior to any distribution of trust assets to (or on behalf of) that beneficiary or person in accordance with the requirements of Regulation 7.

Where a business relationship has been assessed as a high risk relationship, verification of the identity of any beneficiaries must, where possible, be undertaken at the time that the assessment of risk is made. Where it is not possible to do so, the reasons must be documented and signed off by a Director.

All identity documentation MUST be verified in accordance with the Individual Clients section above PRIOR to any distribution payments being made. Identification & Verification – Refer to due diligence requirements in the relevant section of this Manual.

#### 4.6.2 Clients whose ownership involves trust structures

Trusts do not have a separate legal personality and therefore the business relationship is actually conducted through its trustees. DCSL must therefore treat the Trustees as their client along with the trust.

In accordance with the Handbook Rule 139 DCSL must:

- verify the legal status, name and date of establishment of the trust;

- verify the identity of the trustees of the trust (unless they themselves are subject to the Handbook) or are an Appendix C Business (see Appendix C of the Handbook for a definition);

Require the trustee(s) of trust to identify and notify DCSL of the names of the underlying principals and beneficial owners i.e.:

- the settlor(s) (initial and any person subsequently settling funds into the trust);

- any protector(s) or co-trustee(s); and

- any beneficiary with a vested interest or any person who is the object of a power; and
- Understand the nature of the trust structure and the nature and purpose of activities undertaken by the structure sufficient to monitor such activities and to fully understand the business relationship.

Verification of the identity of the underlying principals and beneficial owners must be undertaken either by DCSL by requesting the trustee to provide identification data on them, by way of a certificate or summary sheet (see Appendix B in the Handbook for an example).

**Verification** – In accordance with Rule 140 and to comply with Rule 139 DCSL will obtain the following:

• Certified copies of relevant pages of Trust Deed which confirm the following:

- name of Trust:

- date of establishment;

- name of Trustee(s);

- name of the Protector (if applicable);

- name of the settlor(s); and

- purpose of Trust.

**i.e. DCSL requires a certified extract of Trust Deed showing recitals and signature of Settlor and Trustee(s). The whole Trust Deed should not be requested and if one is received, then it should be returned and only the information as outlined above be retained.**

• Verification of the identity of beneficiaries or any persons who are the object of a power must be undertaken prior to any distribution of trust assets to (or on behalf of) that beneficiary in accordance with the requirements of Regulation 7. Where a business relationship has been assessed as a high risk relationship, verification of the identity of any beneficiaries must, where possible, be undertaken at the time that the assessment of risk is made. Where it is not possible to do so, the reasons must be documented and signed off by a Director.
All identity documentation **MUST** be verified in accordance with the Individual Clients section above **PRIOR** to any distribution payments being made.

• For Trustees regulated by the GFSC or Appendix C equivalent authority (Low Risk) obtain the following:

- copy of relevant authority webpage confirming approval;

- Letter of introduction from the regulated Trustee to DCSL confirming that they have identified and verified the underlying principals and can provide CDD evidence upon request without delay.
  • In the case of a non-regulated Trustee, certified due diligence on:

- Trustees (as per Individuals or legal bodies requirements above);

- Protectors (as per Individuals or legal bodies requirements above);

- Letter of introduction from the Trustee to DCSL confirming that they have identified and verified the underlying principals and can provide CDD evidence upon request without delay.

### 4.7 STANDARD RISK CDD - EMPLOYEE BENEFIT SCHEMES ETC.

In accordance with the Handbook Rule 144, where DCSL provides services to:

- an employee benefit scheme or arrangement;

- an employee share option plan;

pension scheme or arrangement;

- superannuation scheme; or

• a similar scheme where the contributions are made by an employer or by way of a deduction from wages and scheme rules do not permit assignment of a member's interest under the scheme, then DCSL will treat the sponsoring employer, the trustee, the foundation council, and any other person who has control as the business relationship as the principal and identify and verify their identity accordingly (as per requirements for Individuals or Legal Bodies).

### 4.8 STANDARD RISK CDD - FOUNDATIONS

#### 4.8.1 Background

A "Foundation" means:

- a foundation created under the Foundations (Guernsey) Law, 2012 or

- an equivalent or similar body created or established under the law of another jurisdiction
  A Foundation is a legal personality, which is separate and independent from the

Founder. It is a requirement for foundation created under the Foundations

(Guernsey) Law, 2012 to register the Foundation's Charter with the Guernsey Registry. The Charter is a public document. The Charter is not permitted to be a template document and must be bespoke to each Foundation's individual requirements and detail explicitly the purpose of the Foundation and how it is to be administered.

DCSL's fiduciary responsibility is to the Foundation and not the beneficiaries, this is the opposite of DCSL's usual responsibility as trustee of a Trust.

Council Members are appointed under the Charter and will be ultimately responsible for ensuring that the Foundation is operated in accordance with the Foundations Charter and Rules. Council Members should be seen as not to be too incestuous e.g. family members.

The Rules will detail the beneficiaries and their rights, unless named the beneficiaries will have no rights. Rules are not made available for public release. Where disenfranchised beneficiaries are permitted under the Charter, a Guardian will be required to be appointed.

**4.8.2 Clients whose ownership involves Foundations**

When DCSL enters into a business relationship with a client that is a Foundation, it must:
• Identity and verify the identity of the Foundation, including:

- name;

- official identification number (if applicable);

- date and country or territory of registration (if applicable);

- Registered Office;

- principal place of operation/administration (if different from registered office); - Registered Agent (unless they themselves are subject to the Handbook or are an Appendix C Business (see Appendix C of the Handbook for a definition); and - legal status of Foundation.

• require the registered agent, foundation officials or other relevant persons to identify and notify DCSL of the names of the underlying principals and beneficial owners, including: - he Founder(s);

- all Councilors;

- any Guardian;

- any beneficiary including any default recipient; and

- any other person with ultimate effective control over the capital or assets of the legal body.

• understand the nature of the Foundation structure and the nature and purpose of activities undertaken by the structure sufficient to monitor such activities and to fully understand the business relationship.
Before commencement of a business relationship, DCSL must determine

whether any persons listed above within the relationship are to be classified High Risk. If the answer is "Yes" enhanced due diligence requirements will need to be undertaken in accordance with Chapter 5 of The Handbook.

**Verification** – Certified copies of one or more of the following examples are considered suitable to verify the legal status of the foundation:

• Certificate of Registration;

• a Registry Search (if applicable including confirmation that the foundation has not been and is not in the process of being dissolved, struck off, wound up or terminated;

• latest audited Financial Statements;

• charter; or

• council Resolution authorising the opening of the account and recording account signatories

When identifying and verifying the identity of founders, foundation officials, beneficiaries and others DCSL must follow the identification and verification requirements for clients who are individuals and legal bodies as set out earlier in this section.

**4.9 POWERS OF ATTORNEY**

Copies of the Power of Attorney must be maintained by DCSL. An explanation of the reason for granting the Power of Attorney must be held on file.

In order to comply with the Handbook Rules 119 and 131, DCSL must ensure that, prior to issuing a Power of Attorney, DCSL has on file relevant due diligence verification documents (as per Individuals above) on the holders of the Powers of Attorney as well as the Client.

Further investigation must be conducted if there appears to be no evident reason for the granting of a Power of Attorney and such concerns should be escalated to a Director.

A Power of Attorney Register will be maintained and the relevant Administrator is responsible for ensuring this is updated. The Register should state to whom the Power of Attorney is issued, the reason for the Power of Attorney, the date issued and the date of expiry.

General Powers of Attorney are not to be issued and the Powers of Attorney should always have an expiry date (this should be a maximum of one year if it required for longer it should be reissued)

**4.10 SUITABLE CERTIFIERS**

In accordance with the Handbook Rule 103, DCSL must give consideration to the suitability of a certifier based on the assessed risk of the business relationship being undertaken, together with the level of reliance being placed on the certified documentation. DCSL must exercise caution when considering such documents from an unregulated financial services business and the risks associated with the country from where the documents originate.

In accordance with the Handbook Rule 104 DCSL must be satisfied that the certifier is not closely related to the person being identified and whose documents are being certified.

A member of DCSL staff may, where they have met the individual and seen the original documentation, certify copies of identity verification.

In order to comply with The Handbook Rule 104 where DCSL have determined that verification documentation required must be certified, the following are examples of acceptable certifiers:

• member of the judiciary, senior civil servant, serving police or customs officer; • an officer of an Embassy, Consulate or High Commission of the country or territory of issue;

- an Advocate, lawyer or notary public who is a member of a recognised professional body;
- an actuary who is a member of a recognised professional body;
- an accountant who is a member of a recognised professional body;
- member of Institute of Chartered Secretaries and Administrators; or
- Director or officer of an Appendix C (as defined in The Handbook) financial services business or financial service business subject to group/parent policy where the head office is in an Appendix C country/territory. The above list is not exhaustive.

In circumstances where an Introducer has been accepted by DCSL, and has provided all satisfactory Client Due Diligence to DCSL, then such Introducer may be permitted as a suitable certifier, particularly where none of the above persons are available to do so.
For foundations consideration can be given to allowing a Foundation Official to verify the documents and for Companies consideration can be given to accepting certification by a director or the company secretary.

The certifier will need to:

- confirm they have met the individual in person or that the photograph is a true likeness;
- confirm they have reviewed original documentation and that the copy is true and accurate;
- affix signature;
- date their certification;
- confirm their position/status held;
- provide the name of the company they represent; and
- provide adequate information so that contact can be made with them in the event of a query.

**4.11 ELECTRONIC IDENTIFICATION/VERIFICATION**

In accordance with the Handbook, identification data can be obtained from external electronic databases and other sources such as the internet, including information published by Governments. However, this verification information should be considered by DCSL based on the Risk Assessment of the Client. Such sources should be documented by the Administrator for DCSL records and the verification process approved as sufficient by Compliance Support and a Director.

DCSL will utilise numerous websites including World Check in order to assist in its due diligence processes.

**4.12 AGENTS, CONSULTANTS AND ADVISERS**

In order to comply with the Anti-Bribery and Corruption section of this Manual,

DCSL will, upon the appointment of or entering into an agreement with an Agent, Consultant or Advisor, undertake a review of the proposed appointee. This will involve C6/Worldcheck searches, web searches and if so decided by the Directors taking into account the nature of the agreement being entered into, further due diligence may be required.

**4.13 TIMING OF IDENTIFICATION AND VERIFICATION OF IDENTITY**

DCSL is obliged to obtain identification and verification of the identity of any person or legal arrangement. In order to meet Regulations 4 to 6 of the Handbook, DCSL must before or during the course of establishing a new business relationship, identify and where appropriate verify the identity of the client and of any potential beneficial owner or underlying principals.
It is DCSL's policy to obtain all due diligence during the establishment of a business relationship. However, there may be circumstances where DCSL wants to establish a new business relationship without yet having verified identity. This may be done as long as verification is completed as soon as reasonably practicable thereafter and the need to do so is essential not to interrupt the normal conduct of business.

However, this ought to be considered the exception, rather than the rule. In accordance with the Handbook Rule 170, the following must be confirmed before the business relationship can be established and, where verification is outstanding, in order to manage the risks appropriately:

- establishing that it is not a high risk relationship/transaction;
- ensuring that the funds are not passed to third parties;
- monitoring by senior management of these business relationships to ensure verification of identity is completed as soon as reasonably practicable;
- ensuring funds received are not passed to third parties; and
- establishing procedures to limit the number, types and/or amount of transactions that can be undertaken. However, this must only be done on the authorisation of a Director and Compliance Support. All payments made in such circumstances should be notified to Compliance Support who will monitor the business relationship to ensure that verification of identity is completed as soon as reasonably practicable and that the number, types and/or amount of transactions that can be undertaken are limited.

**4.14 FAILURE TO COMPLETE CDD**

In accordance with the Handbook Rule 174, any CDD information which remains outstanding for more than three months following the request for documentation must be referred to Compliance Support. Compliance Support will be responsible for notifying a e Director, who will make the appropriate decision as to whether to pursue the information at a higher level or terminate the relationship. Consideration must be given as to whether the failure to receive the outstanding items gives rise to a suspicion. Any suspicion must be reported to the MLRO or NO.

In accordance with the Handbook Rule 176, where the decision is made not to proceed with the relationship, all funds received for the business relationship MUST be returned to the source from which they came (regardless of whether the source is the client or a third party). If a disclosure has been made to the FIS, the FIS should be consulted and consent sought and obtained before terminating a relationship or returning funds.

**5. ENHANCED DUE DILIGENCE – HIGH RISK RELATIONSHIPS**

**5.1 POLICY**

In accordance with the Handbook, clients with one or more high risk factors as detailed in section 3.5 should normally be classified as high risk and subject to enhanced due diligence.
However, it should be noted that (with the exception of compulsory high risk indicators detailed below) where DCSL does not assess the overall risk as high because of strong and compelling mitigating factors, DCSL must identify the mitigating factors and, along with the reasons for the decision document them.
In such cases the risk rating may be down-graded to standard risk.

Compulsory high risk indicators: any proposed or existing business relationship which either has characteristics identified in Regulations 5(1) (a) to (c) of the Regulations or is connected to any of the countries listed in Part A or Part C of Instructions issued by the Commission. These relationships must be designated high risk.
To meet the enhanced due diligence requirements of the Handbook, DCSL must: • establish the source of funds and source of wealth;

- obtain additional identification data and / or verification documents as considered necessary and/or obtaining additional information to understand the purpose and intended nature of the business relationship; and
- undertake more frequent and extensive monitoring.

**5.2 PROCEDURES**

For relationships assessed as high risk, DCSL will obtain on the principal (i.e. the settlor of a trust or the ultimate beneficial owner of a company):
• Two business references, if possible, one should be from a bank which must be an international bank which has a head office based in an Appendix C country or territory.

The following are examples which might be considered to evidence enhanced due diligence. This list is not exhaustive and other methods may be identified by the Directors in which to fulfil this obligation dependent upon the client.

**5.2.1 Obtain additional identification data**

- Alternative thirds party address verification – e.g. electoral register (in addition to standard address verification), or visit to premises;
- look up employer's website to see if listed as an employee or director;
- look up address on land registry;
- carry out further/more detailed internet searches by experienced staff/persons; or
- request an independent third party report.

**5.2.2 Identify additional aspects of the client's identity**

- Seek confirmation of employment from employer;
- ask for copy of marriage certificate / birth certificate;
- ask for copy of firearms licence or driver's licence (where this has not already been used for verification of identity or address);
- verify professional or academic qualifications said to be held; or
- commission a third party to carry out "deep" due diligence checks on the parties.

**5.2.3 Take reasonable measures to establish the source of any funds and of the wealth of the client and any beneficial owner and underlying principal**

- Ask for copy of will/letter from trustee or executor where wealth is said to be inherited;
- ask for evidence of sale of business or property;
- ask for copies of pay slips, contract of employment (evidencing salary) or evidence verifying payment of bonuses;
- ask for proof of entitlement to rental income (e.g. copy of rent book or records from rental agent); or
- ask for evidence of trades (contract notes or statements) where wealth is said to be derived from such investment activities.

**5.2.4 Obtain additional information in order to understand the purpose and intended nature of the business relationship**

- Ask for copy of contract of sale if potential client is said to have purchased a business;
- ask for copy of a business plan; or
- ask for a third party endorsement of the legitimacy of the proposed business relationship (e.g. copy of statutory exemption or concession for proposed activity).

**5.2.5 Carry out more frequent and more extensive on-going monitoring of the client relationship**

- Implement a periodic review by an administrator (to be decided on a case-by case basis);
- set up Google Alert notifications on client and/or related persons / underlying principals;
- establish requirement for periodic reviews by Compliance Support (to be decided on a case-by-case basis); or
- set-up extra questions / checks for any payments on this account.

**5.2.6 Other measures**

- Limit payments from account to specific persons;
- require additional sign-off from senior management on transactions on the accounts.

**5.3 LEGAL PERSONS ABLE TO ISSUE BEARER INSTRUMENTS**

Where a legal person who is the client, beneficial owner or underlying principal has issued or has the potential to issue bearer shares, bearer warrants or bearer negotiable instruments, DCSL will undertake enhanced due diligence and either seek assurances that such bearer instruments will not be passed on or issued and monitor accordingly, or will itself hold the bearer instruments.

**6. SIMPLIFIED / REDUCED CDD – LOW RISK RELATIONSHIPS**

**6.1 POLICY**

Chapter 6 of the Handbook provides for circumstances where reduced or simplified due diligence may be obtained where the risk of money laundering or terrorist financing has been determined as being low. Some examples would be a locally (Guernsey) resident individual whom DCSL meets face-to-face investing into a low risk product or where information on the identity of the client, beneficial owners and underlying principals is either publicly available, or where adequate checks and controls exist elsewhere in national systems.
The examples given in the Handbook are as follows:

- Individuals who are Guernsey residents
- Legal bodies quoted on a regulated market
- Appendix C business

- Non-Guernsey Collective Investment Schemes
- Intermediary Relationships (but see below)

It should be noted that, where DCSL has reason to believe that any aspect of the relationship could be other than low, then simplified or reduced CDD measures must not be applied.

**6.2 INDIVIDUALS MET FACE TO FACE BY DCSL STAFF**

Note that this refers to Guernsey residents only who are establishing a business relationship with DCSL. In such cases, the following identification data as a minimum must be obtained:

- legal name, any former names (such as maiden names) and any other names used;
- principal residential address;
- date of birth; and
- nationality.

Verification of identity must be obtained on the legal name. This can be achieved by obtaining certified true copy;

· passport;

· ID card;

· armed forces ID card;

· current Guernsey driving licence bearing a photograph; or

· independent data sources (including electronic sources).

DCSL must also either verify the principal residential address or the date of birth of the individual, this can be undertaken by obtaining certified true copies of one of the following:

- Bank/credit card statements or utility bills (no more than 3 months old are acceptable. Mobile phone bills are not acceptable);
- Correspondence from an independent source e.g. central or local Government department or Agency (this will include States departments or Parish Authorities);
- Commercial or electronic databases ;
- lawyer's confirmation of a property purchase;
- personal visit to the residential address;
- an electoral roll; or
- a birth certificate.

While not strictly required for low risk relationships, DCSL will obtain a duly completed and signed Client Acceptance Form.

There is no requirement to obtain references for clients rated as low risk.

**6.3 COMPANIES**

Where a company is a:

- a collective investment scheme regulated by the GFSC;

- is quoted on a regulated market (as defined in section 9 of the Insider Dealing (Securities and Regulated Markets) Order, 1996 as amended); or

- is a wholly owned subsidiary of a company quoted on a regulated market. DCSL must confirm that fact and verify the identity of the authorised signatories who have authority to instruct DCSL. Verification of such individuals must be in accordance with DCSL's policy on identity verification for individuals as per section 4.4.

**7. MONITORING TRANSACTIONS AND ACTIVITY**

**7.1 ONGOING MONITORING POLICY**

DCSL staff have an obligation to monitor DCSL's clients and to scrutinise unusual, complex or high risk transactions or activity so that money laundering or terrorist financing may be identified and prevented.
For all clients, DCSL will scrutinise transactions or other activity, with special regard to:

- complex transactions,

- transactions which are both large and unusual, and

- unusual patterns of transactions.

This may involve requesting additional information during the life of the business relationship. If the client or his/her representative is reluctant to provide information to explain unusual transactional behaviour, DCSL staff should persevere and the MLRO, NO and/or any Director will be available to help persuade potential clients to provide this information.

On-going monitoring of clients carried out as part of the business relationship is one of the most important aspects of effective on-going CDD procedures. Staff can usually only determine when they might have reasonable grounds for knowing or suspecting that money laundering or terrorist financing is occurring if they have the means of assessing when a transaction or activity falls outside their expectations for a particular client. An unusual transaction or activity may be inconsistent with the expected pattern of activity for a client. This may indicate money laundering or terrorist financing activity where the transaction or activity has no apparent economic or visible lawful purpose. It is up to all DCSL staff to make enquiries to satisfy themselves over the reason for unusual activity and record any findings on file. They must also ensure that the transactions and activities being conducted are consistent with DCSL's knowledge of the client, their business, location, source of funds and source of wealth.

The requirement to conduct on-going monitoring helps to ensures that DCSL is aware of any changes in the development of the business relationship. It is important to note that, as the business relationship develops, the risk of money laundering or terrorist financing may change.

All payments to and from DCSL must either be to its clients or to other reputable service providers.

### 7.2 EDD, MORE EXTENSIVE ONGOING MONITORING

Monitoring of transactions is risk-based and therefore more extensive on-going scrutiny is undertaken for high risk clients than previously outlined for the ongoing monitoring requirements of standard risk rated clients of DCSL. This enhanced monitoring will include:

• scrutiny of transactions involving high risk clients to ensure that the transactions and activity being conducted are consistent with DCSL's knowledge of the client, their source of funds and source of wealth. This will involve all such transactions being authorised by a director of DCSL;

• all high risk relationships will be subject to more frequent periodic reviews by operational staff. The Board has agreed that high risk structures are reviewed annually, medium risk every two years and low risk, every three years;

• high risk clients are subject to dual Director sign off as well as sign off by the Compliance Support.
Compliance Support will undertake periodic reviews on client relationships which are placed on the "Watch list" e.g. clients being monitored by the Directors and such reviews will be reported to the Directors.

### 7.3 COMPLIANCE REVIEW

Regulation 2 of the 2007 Regulations requires the Board to take responsibility for establishing and maintaining a policy for the review of DCSL's compliance with the Regulations. The Board have resolved that such a review should be carried out annually, or more frequently where there are material amendments to the 2007 Regulations.

DCSL will ensure that sufficient time will be made available to Compliance

Support to enable them to carry out their duties and responsibilities. Compliance Support will have access to all of DCSL's files and should receive full cooperation from all staff. Compliance Support will report to the Board at least at every routine Board meeting and has full and free access to the Managing Director and the Board at all times.

## 8. REPORTING SUSPICION

### 8.1 POLICY

DCSL has appointed a MLRO. All suspicions will be reported to the MLRO or the NO in the MLRO's absence. Only the MLRO or NO will make suspicious
transaction reports to the FIS.

### 8.2 RECOGNITION OF SUSPICIOUS TRANSACTIONS OR ACTIVITY

A suspicious transaction will often be one which is inconsistent with a client's entity's regular activity or with the normal business for a company or trust.
Examples are as follows:

· any unusual financial activity of the client in the context of his normal, expected activities;
· any unusual transaction in the course of a usual financial activity;

· any unusually-linked transactions;

· any unusual employment of an intermediary in the course of a usual transaction or financial activity;
· any unusual or disadvantageous early redemption of an investment or breaking of a deposit.
· any unusual method of payment - third party payments are classified as unusual methods of payment.
However, a suspicion need not only be based on transactions or activity of the business relationship, as information may arise from other sources e.g.

- media;
- intermediaries;
- authorities; or
- client/underlying principals themselves.

An employee is obligated to report any suspicion to the MLRO regardless of the amount involved.
The MLRO will promptly review, consider and acknowledge each such internal report and determine whether it results in there being a knowledge or suspicion or reasonable grounds for knowing or suspecting that someone is engaged in Money Laundering or Terrorist Financing. Where the MLRO has determined that an internal report does result in there being such knowledge or suspicion or reasonable grounds for knowing or suspecting that someone is engaged in money laundering or terrorist financing (including where such suspicion and knowledge or reasonable grounds for such suspicion or knowledge is identified during the Client Due Diligence process) he will make a disclosure to the FIS. Although DCSL is not expected to conduct investigations which would be carried out by the law enforcement agencies, DCSL must in accordance with the Handbook Guidance paragraph 300, act responsibly and ask questions to satisfy its queries or understand a particular transaction or activity or proposed activity.
If in doubt refer to MLRO.

**8.3 SUSPICIOUS FEATURES OR ACTIVITIES – TRUSTS AND COMPANIES**

It is DCSL's responsibility to understand the purpose and activities of the structures it acts as trustee to. If DCSL is unable to do so, then it should seek further information. If it is still unable to understand the purpose or activities, it should consider whether a suspicion is raised with regards to the activities being conducted or and consider if the assets of the entity could be the proceeds of crime or intended for terrorist financing.
If DCSL is unable to obtain an adequate explanation of the following or any other feature which causes concern, a suspicion could be raised:

- overly complex network of trusts and/or nomineeships and or/Companies; • transactions which lack economic purpose (for example, sales or purchases at undervalued or inflated prices, payments or receipt being split between large number of bank accounts or other financial services products, companies consistently making substantial losses;
- transactions which are inconsistent (for example in size or source) with the expected objectives of the structure;
- arrangements established with the apparent objective of tax evasion;
- structures or transactions set up or operated in an unnecessarily secretive way, for example involving "blind" trusts, bearer shares, endorsed cheques, cash or other bearer instruments or use of P.O. Boxes;
- lack of clarity about beneficial owners or interests or difficulties in verifying identity of persons with ownership or control;
- unwillingness to disclose the source of assets to be received by a trust or company;
- unwillingness for the fiduciary to have the degree of information and control which it needs to fulfill its duties;

- underlying entities operated outside the control of the Trustees/Directors e.g. certain types of trading companies.

DCSL should consider whether these or other features cause suspicion or reasonable grounds for suspicion. Documentary evidence of records and explanations received must always be retained in accordance with the record keeping policy.
DCSL should in addition to obtaining adequate CDD (prior to or during the establishment of the relationship) continue on an ongoing basis to monitor the activities and structures to which it provides services.

**8.4 REPORTING OF SUPICIOUS TRANSACTIONS OR ACTIVITY**

If a member of staff forms a suspicion in relation to a transaction, a report plus comprehensive back up documentation to evidence such suspicion must be made and filed with the MLRO or in his absence, the NO. If the MLRO decides that a disclosure should be made, the MLRO will make a disclosure to the FIS via Themis, the online reporting facility available on the website of the FIU, at www.guernseyfiu.gov.gg. A copy of the prescribed online form is set out in Appendix D2 of the Handbook. The FIS will acknowledge receipt of the disclosure. The MLRO will need consent from the FIS to continue to transact in respect of the business relationship(s) connected to the suspicious activity report.

The MLRO is obligated under the Handbook Rule 301 to inform the FIS of any subsequent, relevant information or documentation received. Reporting via Themis to the FIS by the MLRO should be completed by no later than 48 hours following receipt of the completed internal reporting form and sufficient supporting information. This should allow the MLRO sufficient time to consider the internal report and whether it requires onward reporting to the FS. The MLRO is obligated to determine in accordance with the Handbook Rule 304, under which law the disclosure is being made. Reports of suspicion of money laundering
(including drug money laundering) must be disclosed under the provisions of the DL and suspicions relating to terrorism must be disclosed under the T&CL. Should the MLRO in accordance with the Handbook Rule 301, decide that a disclosure is not appropriate then the MLRO will compile a statement as to why it was not filed with the Financial Intelligence Service and retain that statement along with the records of the internal report.

In accordance with the Handbook Rule 313, the MLRO will retain all reports received and a register which will disclose whether or not an external report was forwarded to the FIS. The reasons for not disclosing will be documented and retained. The register contains details of:

- date of Disclosure;
- the person who made the disclosure;
- the person to whom the disclosure was forwarded; and
- reference by which supporting evidence is identifiable.

In accordance with the Handbook Rule 314, DCSL must consider whether the suspicion which has been triggered is such that all of the assets of the business relationship are potentially suspect. Where DCSL cannot distinguish the assets which are suspicious from legitimate funds, DCSL will need to carefully consider all future transactions or activities and the nature of continuing the relationship and in the light of the findings implement an appropriate risk based strategy. Once a suspicion is formed it is a criminal offence either not to report the suspicion or to tip off anyone of the suspicion. Tipping off can be done inadvertently; for example, by telling the client that a report has been made on them or that an investigation is being carried out when asking further questions of a client in order to gain further information.

Once a suspicion is formed and a report has been made to the MLRO/NO, then the Directors will have to decide

if they wish to continue with the business relationship. If not, then any attempt to exit a relationship on which a report has been made must be carried out with the express knowledge and consent of the FIS.

In all cases where a report has been made, the MLRO will monitor such persons accordingly.

## 9. TRAINING

### 9.1 STAFF AND INTRODUCER TRAINING

9.1.1 On an at least an annual basis DCSL will provide ongoing AML/CFT training to all staff and Introducers in particular covering:

- DCSL's customer due diligence requirements
- the requirements for the internal and external reporting of suspicion;
- the criminal and regulatory sanctions in place for failing to report information in accordance with policies, procedures and controls;
- the identity and responsibilities of the MLRO;
- the principal vulnerabilities of the products and services offered by DCSL; and • new developments, including information on current money laundering and terrorist financing techniques, methods, trends and typologies.

9.1.2 Such training will be held more frequently if new legislation or significant changes to the Handbook are introduced or where there have been significant technological developments within DCSL.

9.1.3 External compliance resources will ensure that the Board and senior management of DCSL receive additional training in:

- the relevant enactments and the 2007 Regulations and information on the offences and related penalties, including potential director and shareholder liability;
- the CDD and record keeping requirements; and
- the internal and external suspicion reporting requirements.

## 10. RECORD KEEPING

### 10.1 GENERAL

As a minimum DCSL must keep the following records:

- copies of the identification data obtained to verify the identity of all clients, beneficial owners and underlying principals;
- copies of any client files, account files, business correspondence and information relating to the client relationship;

records of all transactions carried out on behalf of or with a client in the course of business, both domestic and international. In every case, sufficient information must be recorded to enable the reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity;

- DCSL's reviews of unusual, complex and high risk transactions;
- copies of initial and subsequent Relationship Risk Profiling forms, including consideration of exposure to Bribery and Corruption; and
- copies of periodic client reviews.

**10.2 TRANSACTION RECORDS**

With reference to record keeping requirements for transactions, documentation must be maintained which includes:

- the name and address of the client(s), beneficial owner and underlying principal;
- the currency and amount of the transaction;
- account name and number;
- details of the counterparty, including account details;
- the nature of the transaction; and
- the date of the transaction.

**10.3 REPORTING SUSPICION**

DCSL will keep records of:

- any internal suspicion report;
- records of actions taken under the internal and external reporting requirements; • when the MLRO has considered information or other material concerning possible money laundering or terrorist financing, but has not made a disclosure of suspicion to the Financial Intelligence Service, a record of the other material that was considered and the reason for the decision; and
- copies of any disclosures made to the Financial Intelligence Service

**10.4 TRAINING RECORDS**

Compliance Support will retain records of:

- the dates AML/CFT training was provided;
- the dates Bribery and Corruption training was provided
- the nature of the training; and

- the names of the staff who received training.

This information will be kept in a training register maintained by Compliance Support.

**10.5 COMPLIANCE**

Compliance Support will retain a central file containing records of:

- reports by the MLRO and Compliance Support to the Board;
- records of consideration of those reports and of any action taken as a consequence;
- any records made within DCSL or by other parties in respect of compliance of DCSL with the 2007 Regulations and the Handbook; and
- all AML/CFT correspondence with the GFSC or any other regulator (this will by the end of 2015 be all via the online portal of the GFSC), the FIS, Law Officers of the Crown, law enforcement body or judicial body.

**10.6 DOCUMENT RETRIEVAL**

Compliance Support will periodically carry out checks on a sample of files to ensure that electronically maintained and paper documentation is readily
retrievable.

Compliance Support will ensure that this sample includes documents held by third parties (such as introducers).

It is a requirement of the 2007 Regulations that any documents which must be retained are made available promptly to domestic (Guernsey) competent authorities where so requested under the 2007 Regulations or other relevant enactment.

**10.7 RECORD RETENTION PERIODS**

For AML/CFT purposes DCSL shall retain the following documents for at least 5 years (or such other longer period as the GFSC may direct):

a) client due diligence information - from the date the business relationship ceased;
b) a transaction document -from the date that both the transaction and any related transaction were completed;
c) copies of suspicious transaction/activity reports made to the MLRO and those made to the FIS - from the date the business relationship ceased; (d) details of any AML/CFT training carried out – from the date the training was carried out;
d) minutes or other documents prepared before, during and after a review at a Board meeting (as required under Regulation 15(c)) of DCSL's compliance with the 2007 Regulations – from the date they were finalised. However, where such minutes or other records are superseded by later minutes or other documents prepared under Regulation 15 (c) more than 5 years from the date the first documents are prepared then the documents and minutes should be kept for that longer period); and
e) policies, procedures and controls which DCSL is required to establish and maintain pursuant to the 2007 Regulations - from the date that they ceased to be operative.

## 11. ANTI-BRIBERY AND CORRUPTION

### 11.1 INTRODUCTION

In March 2013 the GFSC added Chapter 13 to its AML/CFT Handbook devoted entirely to the risks to a financial services business of bribery and corruption. It should be noted that both bribery and corruption are already predicated offences under section 1(1) of the All Crimes Law. DCSL will consider these risks in its day to day administration and management of trust and company structures and the specific procedures listed should ensure that DCSL meets the requirements and guidance contained in Chapter 13.
A bribe is an inducement or reward offered, promised or provided in order to gain any commercial, contractual, regulatory or personal advantage.

Corruption is an abuse of a position of trust in order to gain an undue advantage In relation to DCSL as a financial services business, bribery and corruption risks can be those risks directly linked to DCSL's business, any person acting on behalf of DCSL's business, or any third party connected to a business relationship to which DCSL provides regulated activities.

### 11.2 ABC RISK ASSESSMENT

In order to understand the exposure to bribery and corruption risks faced by DCSL, it must ensure its AML/CFT risk assessment take account of the risks that is posed by the specific offences of bribery and corruption. DCSL will use the examples given in paragraph 378 of The Handbook as its guidance. Where any additional risks are highlighted these will be added to the existing AML/CFT risk assessment (as allowed under paragraph 377 of The Handbook) along with the mitigating factors.

DCSL's AML/CFT risk assessment will be reviewed at least annually and will also include in that review consideration of the specific risks of bribery and corruption.

### 11.3 THE BOARD OF DCSL

The Board of DCSL is ultimately responsible via DCSL's risk framework, to ensure the business complies with the Guernsey Corruption Law (see below for a summary of this Law). The Board also need to be aware of other relevant legislation concerning bribery and corruption (namely the UK Bribery Act 2010)
The Board need to ensure that DCSL has:

- established policies, procedures and controls with regard to ABC;
- reviewed its compliance with the policies, procedures and controls in place with regard to ABC;
- a procedure to consider, at regular intervals, the appropriateness and effectiveness of the ABC policies, procedures and controls and take the necessary action to remedy any identified deficiencies; and
- It has taken appropriate measures to keep up to date with, and keep abreast of, bribery and corruption issues.

In order to demonstrate that DCSL will implement "adequate procedures" as required in the UK Bribery Act 2010, to prevent corrupt practices internally or by third parties on their behalf, The Company will operate the following principles:
· proportionate Procedures set by DCSL;

· commitment by the Board to foster a culture where bribery is not acceptable; · Risk Assessment of bribery and corruption risks which must be reviewed annually (see ABC Risk Assessment section above);

· Due Diligence on employees and agents and a clear process around receiving money from and paying money to third parties;
· communication (including training) of DCSL policies as detailed above; and

· monitoring and review of these policies and procedures.

**11.4 GIFTS AND ENTERTAINMENT**

Whilst emphasising that Bribery is not tolerated, it is also important to note that in order to conduct business there will be a need to both give and receive entertainment and gifts. It is not practical to put finite monetary amounts on what will and will not be acceptable levels of gifts and entertaining as the country, the culture and the circumstances will define what is and is not acceptable.
As a policy DCSL will monitor and record all gifts given and received in excess of £100 and hospitality given or received in excess of £200. All gifts and entertainment over £300 must be specifically approved in advance by the Managing Director and, in the case of the Managing Director, another Director. It is not acceptable for an employee (or someone on their behalf) to:

• Give; promise to give, or offer, a payment, gift or hospitality with the expectation or hope that a business advantage will be received, or to reward a business advantage already given.

• Give, promise to give, or offer, a payment, gift or hospitality to a government official, agent or representative to "facilitate" or expedite a routine procedure. • Accept payment from a third party that the employee knows or suspects is offered with the expectation that it will obtain a business advantage for them.

• Accept a gift or hospitality from a third party if the employee knows or suspects that it is offered or provided with an expectation that a business advantage will be provided by us in return.

• Threaten or retaliate against another employee who has refused to commit a bribery offence or who has raised concerns.

**11.5 FACILITATION PAYMENTS AND KICKBACKS**

Facilitation payments are typically small, unofficial payments made to secure or expedite a routine government action by a government official.

Kickbacks are typically payments made in return for a business favour or advantage. DCSL staff must avoid any activity that might lead to or suggest that a facilitation payment or kickback will be made or accepted by DCSL. For the avoidance of any doubt, DCSL does not make, and will not accept, facilitation payments or "kickbacks" of any kind.

**11.6 GENERAL MONITORING AND AWARENESS**

The reasons for all payments should always be considered as well as whether the amounts requested are proportionate to the goods or services provided. Invoices or receipts which detail the reason for the payments should be obtained and kept on the relevant company's file.

DCSL staff should monitor and be aware of any transactions or activities that do not have any apparent economic or visible lawful purpose.

For example, consideration should be given to the following:

• commission structures, e.g. considering whether commission percentages paid to introducers of new business are reasonable, proportionate and transparent;

- charitable or political donations and sponsorship;
- instructions to effect payments for advisory and consulting activities with no apparent connection to the known activities of the business;
- payments to unknown third parties; and
- effecting transactions through cash payments and money orders.

If any suspicions, concerns or queries regarding a payment or activity arise, you should liaise with the MLRO.

**11.7 ABC – POLICIES, PROCEDURES AND CONTROLS**

In addition to the above:

- DCSL application and take on forms will include reference to bribery and corruption risks;
- the relationship risk profiling forms will include these risks;
- the client file reviews and general monitoring process will include reference to considering bribery and corruption risks;
- training on bribery and corruption will be undertaken for all staff. In addition,

DCSL employees that are responsible for the implementation and monitoring of ABC policies, procedures and controls will need to have additional training to ensure they are competent to evaluate the effectiveness of and any revisions to those policies, procedures and controls; and

- ABC records are to be maintained for the minimum retention period as set out in procedures in this section.

**11.8 THE BRIBERY ACT 2010**

The Act came into force in the UK on 1 July 2011 and consolidates previous legislation into one statute (which is similar to legislation in Guernsey and other jurisdictions). The Act applies to all British Nationals anywhere in the world and creates four offences. The first three are equivalent to those in Guernsey and other jurisdictions:

· An offence by an individual, to offer, promise or give a bribe.

· An offence by an individual to request, agree to receive or accept a bribe. · An offence by an individual to offer, promise or give a bribe to a foreign public official to obtain or retain business.

· An offence by the company where the company fails to prevent bribery by those acting on its behalf. The company will be liable even if there is no negligence or guilt from the board and senior management, but it is a defence if it can be shown that it had “adequate procedures” in place to prevent bribery.

A company commits an offence if a person associated with it bribes another person for the company's benefit. A person is "associated" with a company if such person performs services for or on behalf of the company, regardless of the capacity in which it does so. This will therefore be construed broadly and is likely to cover agents, employees, subsidiaries, intermediaries, joint venture partners, main subcontractors and suppliers, all of whom could render a company guilty of this offence.

**11.9 THE GUERNSEY CORRUPTION LAW**

DCSL is subject to the above law and whilst it is similar to the Act, in respect of the criminalisation of corruption, the Act is specific in its requirements to put into place adequate procedures and measures to prevent bribery and corruption.

Therefore, DCSL will meet the Act's requirements as set out above.

**11.10 WHISTLEBLOWING**

DCSL is committed to ensure that any incident of work place fraud or mismanagement is prevented wherever possible and issues identified are dealt with immediately. Any staff member who has reasonable grounds to believe that an incident of work place malpractice or mismanagement has occurred, is occurring or is likely to occur within DCSL are able to raise their concerns either directly to the Managing Director or to the MLRO or external compliance resources. DCSL will encourage employees to raise their concerns about any incidents of malpractice in the work place at the earliest possible stage.
Definition of Malpractice

For the purposes of this policy, DCSL considers the following matters to constitute malpractice;
· commission of a criminal offence;

· incidents of bribery;

· failure to comply with a legal/statutory obligation;

· occurrence of a miscarriage of justice;

· endangerment of the health and safety of any individual;

· damage to the environment;

· the deliberate concealment of any information indicating any of the matters set out above.

**12. SANCTIONS**

**12.1 THE TERRORIST LAW**

The Terrorist Law implements United Nations Security Council Resolution 1373 and Council Regulation (EC) No 2580/2001. This EU Regulation imposes restrictive measures directed against persons or entities (Designated Person) in view of combating terrorism.
The Terrorist Law prohibits DCSL from:

- dealing with funds or economic resources owned, held or controlled by a designated person;

- knowing or having reasonable cause to suspect such funds or economic resources are being dealt with;
- making funds or financial services available (directly or indirectly) to a designated person;
- knowing or having reasonable cause to suspect, the funds or financial services are being made so available;
- making funds or financial services available to any person for the benefit of a designated person;
- knowing or having reasonable cause to suspect the funds or financial services are being made so available;

- making economic resources available (directly or indirectly) to a designated person;
- knowing or having reasonable cause to suspect that the economic resources are being made so available, and that the designated person would be likely to exchange the economic resources, or use them in exchange, for funds, goods or services;
- making economic resources available to any person for the benefit of a designated person;
- knowing or having reasonable cause to suspect, that the economic resources are being made so available;
- intentionally participating in activities, knowing that the object or effect of such activities (whether directly or indirectly) is to circumvent or facilitate the contravention of any of the above prohibitions.

A Designated Person as defined in paragraph 388 of the Handbook means:

- a person designated by Policy Council under the Terrorist Law;

- a person designation under and within the meaning of the UK's Terrorist AssetFreezing etc. Act 2010; or

- a natural legal person, group or entity included in the list provided for by Article 2(3) of Council Regulation (EC) No 2580/2001 of 27 December 2001 on specific restrictive measures directed against certain persons and entities with a view to combating terrorism (as that Regulation is amended from time to time). In order to determine whether a settlor or potential beneficiary is a designated person DCSL reviews all clients, settlors or potential beneficiaries against a full list of financial sanction targets (which DCSL will undertake by reviewing against external sources such as Worldcheck or C6).

Ongoing monitoring is to be performed by Compliance Support who will check the DCSL Viewpoint Database against designated persons and sanctions lists issued by HM Treasury via the subscription facility and periodically scan the DCSL Viewpoint Database against the appropriate monitor.

**12.2 THE AL-QAIDA ORDINANCE**

The Al-Qaida Ordinance implements UN Security Council Resolution 1267 and Council Regulation (EC) No. 881/002. The Resolution and EU Regulation as initially enacted, applied to parties associated with both the Taliban and Al-Qaida. The United Nations Security council passed a Resolution and transferred the list of parties associated to a new regime specific to Afghanistan. In order to comply with the UN regulation, Guernsey issued this Ordinance, which currently remains in force.

A Designated Person as defined in Rule 386 of the Handbook means:

- individuals associated with Al-Qaida; or

- entities and other group and undertaking associated with Al-Qaida.

A full list of Designated Persons is contained in Annex 1 to the EU Regulations.

In order to determine whether an investor is a designated person DCSL reviews all clients, settlors or potential beneficiaries against a full list of financial sanction targets (which DCSL undertakes by reviewing against C6).

Ongoing monitoring is performed by Compliance Support who manually checks the DCSL Viewpoint Database against lists issued by HM Treasury and periodically scans DCSL Viewpoint Database against C6 Monitor.

DCSL acknowledges that under the Terrorist Law and Al-Qaida Ordinance, it is a criminal offence for DCSL to fail to disclose to the Policy Council its knowledge or suspicion that a client, settlor or potential beneficiary is a Designated Person or has committed any of the offences set out in the Law or Ordinance. This requirement is additional to any reporting obligation in the Disclosure Law and the Terrorism and Crime Law.

**12.3 SANCTIONS REGIME - GUERNSEY**

Guernsey's Sanctions Committee co-ordinates sanctions activities, ensures information is distributed publicly and provide advice on sanctions. The Committee reports to the External Relations Group of the Policy Council and Guernsey's AML/CFT Advisory Committee. The Group also works with HM Treasury and the UK's Foreign and Commonwealth Office.

The External Relations Group is mandated on behalf of Policy Council to:

- agree to implement new sanctions measures;

- licence frozen funds; and

- administer notifications and authorisations (e.g. those under the Iran (Restrictive Measures) (Guernsey) Ordinance, 2010).

In addition to the sanctions regime implemented by the terrorist asset freezing enactments, Guernsey has enacted legislation to implement a wide range of country-specific sanctions. The Sanctions are used increasingly for enforcing foreign policy by in order to maintain or restore international peace and security and are often used as an alternative to force.
The United Nations and the European Union are the key bodies who adopt sanctions measures which may include:

- financial sanctions including asset freezes and investment bans;

- travel bans;

- import and export bans;

- arms embargos; or

- trade restrictions.

Though Guernsey's sanction regime is based on legislation and broadly mirrors equivalent UK legislation it is completely separate from and operates independently of the UK.

On occasions, trans-jurisdictional issues may arise at times and transfers of funds will be made to or from another jurisdiction that operates a sanctions regime. In such circumstances a licence, authorisation, or notification may be required in both jurisdictions. Legislative frameworks of some jurisdictions contain provisions that have extra-territorial effect, so may apply to some of the parties involved in a Guernsey transaction on the grounds of nationality or place of incorporation even if the jurisdiction in question is not involved in that transaction.

In such circumstances Compliance Support or the Directors will liaise with the Policy Council to obtain such authorisations.

**12.4 SANCTIONS REGIME - USA**

DCSL must also be aware of any OFAC regulations which can be applied to the following:

- U.S. citizens and permanent resident immigrant regardless of where they are located;
- persons and entities within the United States;

- persons and entities trading in U.S. Dollars;
- U.S. incorporated entities and their foreign branches;
- in the cases of certain sanctions, such as those regarding Cuba and North Korea, all foreign subsidiaries owned or controlled by U.S. companies; and
- foreign persons in possession of U.S. origin goods in some cases.

**13. 'APPENDIX C' BUSINESS**

An Appendix C business is:

· a financial services business supervised by the GFSC; or

· a business which is carried on from

- a country or territory listed in Appendix C to the Handbook and which would, if it were carried on in the Bailiwick, be a financial services business; or
- the United Kingdom, the Bailiwick of Jersey, the Bailiwick of Guernsey or the Isle of Man by a lawyer or accountant; and, in either case is a business

· which may only be carried on in that country or territory by a person regulated for that purpose under the law of that country or territory?
· the conduct of which is subject to requirements to forestall, prevent and detect money laundering and terrorist financing that are consistent with those in the Financial Action Task Force Recommendations on Money Laundering in respect of such a business; and
· the conduct of which is supervised for compliance with the requirements referred to in subparagraph (B), by the GFSC or an overseas regulatory authority. Where the client is an Appendix C business and the purpose and intended nature of the relationship is understood, verification of identity of the Appendix C business is not required. Similarly, where a person authorised to act on behalf of a legal body or legal arrangement is acting in the course of employment by an Appendix C business, then it is not necessary to verify the identity of the Appendix C business or such persons. However, DCSL does require a copy of relevant authority webpage confirming approval of the Appendix C business.

Where an Appendix C Business is acting for underlying principals then verification of identity is required to be carried out by DCSL on those individuals, legal persons or legal bodies as detailed in the relevant section. DCSL will always be providing regulated services to underlying principals therefore DCSL would not be able to merely rely on verifying the Appendix C businesses.

**The following countries are listed as Appendix C countries in the Handbook:**

| | |
|---|---|
| Australia | Finland |
| Austria | France |
| Belgium | Germany |
| Bermuda | Gibraltar |
| Bulgaria | Greece |
| Canada | Hong Kong |
| Cayman Islands | Hungary |
| Cyprus | Iceland |
| Denmark | Ireland |
| Estonia | Isle of Man |
| Italy | Norway |
| Japan | Portugal |
| Jersey | Singapore |
| Latvia | Slovenia |
| Liechtenstein | South Africa |
| Lithuania | Spain |
| Luxembourg | Sweden |
| Malta | Switzerland |
| Netherlands | United Kingdom |
| New Zealand | United States of America |

DOMINION
CAPITAL STRATEGIES


**Europe / Africa / Middle East**
**+44 (20) 4538-2535**

**Latin America & The Caribbean**
**+1 (786) 442-3253**

**Asia & The Pacific**
**+65 3129-5213**

**Dominion Capital Strategies Limited**
**First Floor, Mill Court, La Charroterie**
**St Peter Port, GY1 3PU**
**Guernsey**

**Dominion Capital Strategies Corporate Administration (EPIC-FS)**
**Windsor House, Le Pollet Street. Suites 7 & 8 - 4th Floor**
**St Peter Port, GY1 1WF**
**Guernsey**

**Dominion Asset Management Limited**
**20 Little Britain**
**London, EC1A 7DH**
**United Kingdom**

**Dominion IT Development Hub (DCS SA)**
**Rambla República de México 6205**
**Montevideo, 11600**
**Uruguay**