ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM (AML/CFT) POLICY AND PROCESS: G - 02
GLOSSARY OF TERMS USED IN THE POLICY ............................................. 4
1. INTRODUCTION ...................................................................................... 5
2. DMCC’S COMMITMENT ......................................................................... 5
3. POLICY CUSTODIAN ............................................................................. 6
4. PURPOSE AND RATIONALE ................................................................. 6
5. POLICY STATUS AND SCOPE .............................................................. 6
6. PROCEDURES AND CONTROLS (GENERAL) ........................................ 6
7. PERIODICAL REVIEW ........................................................................... 7
8. IDENTIFICATION (ID), VERIFICATION (VR) AND KNOW-YOUR-CUSTOMER (KYC) ............................................................. 7
9. KYC INFORMATION UPDATING ............................................................. 9
10. AUTOMATED ACTIVITY MONITORING ........................................... 9
11. REPORTING OF SUSPICIOUS ACTIVITIES ......................................... 9
12. TRAINING AND AWARENESS ............................................................ 10
13. RECORD KEEPING ............................................................................... 10
14. DMCC MANAGEMENT AND STAFF RESPONSIBILITIES ............... 11
15. REFERENCES ........................................................................................ 11
APPENDICES ............................................................................................ 12
APPENDIX A – CORPORATE KYC CHECKLIST ..................................... 13
APPENDIX B – INDIVIDUAL SHAREHOLDER KYC CHECKLIST ...... 15
APPENDIX C – CORPORATE KYC UPDATING CHECKLIST .................. 17
APPENDIX D – INDIVIDUAL SHAREHOLDER AND / OR MANAGER KYC UPDATING CHECKLIST ...................................................... 18
**GLOSSARY OF TERMS USED IN THE POLICY**

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AML</td>
<td>Anti-Money Laundering</td>
</tr>
<tr>
<td>AMLSCU</td>
<td>Anti-Money Laundering &amp; Suspicious Cases Unit – Based at the Central Bank of UAE</td>
</tr>
<tr>
<td>CDD</td>
<td>Customer Due Diligence</td>
</tr>
<tr>
<td>CFT</td>
<td>Combating the Financing of Terrorism</td>
</tr>
<tr>
<td>CIBO</td>
<td>Client Identification and Beneficial Ownership</td>
</tr>
<tr>
<td>DFSA</td>
<td>Dubai Financial Services Authority</td>
</tr>
<tr>
<td>DMCC</td>
<td>Dubai Multi Commodities Centre</td>
</tr>
<tr>
<td>ESCA</td>
<td>Emirates Security &amp; Commodities Authority</td>
</tr>
<tr>
<td>FATF</td>
<td>Financial Action Task Force</td>
</tr>
<tr>
<td>FT</td>
<td>Financing of Terrorism</td>
</tr>
<tr>
<td>ID</td>
<td>Identification</td>
</tr>
<tr>
<td>INTERPOL</td>
<td>International Police Organization</td>
</tr>
<tr>
<td>IOSCO</td>
<td>International Organization of Securities Commissions</td>
</tr>
<tr>
<td>KYC</td>
<td>Know Your Customer</td>
</tr>
<tr>
<td>ML</td>
<td>Money Laundering</td>
</tr>
<tr>
<td>NID</td>
<td>National Identification card</td>
</tr>
<tr>
<td>SAR</td>
<td>Suspicious Activity Report</td>
</tr>
<tr>
<td>VR</td>
<td>Verification</td>
</tr>
</tbody>
</table>
1. INTRODUCTION

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

For the purpose of this policy (“the Policy”):

**Money Laundering** is:

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

**The Financing of Terrorism** is:

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

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

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

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

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

1.3. Art 22 (7) of Rule No. 4 of 2002 Re. Organizing Operations at DMCC stipulates that any activities that violate the laws of the State including money laundering are prohibited. Under this law, DMCC is obligated to establish a set of policies and procedures to ensure that neither its members (“Members”) nor its subsidiaries facilitate money laundering and/or the financing of terrorist activities. These laws are more particularly set out in section 15.

2. DMCC’S COMMITMENT

2.1. As a responsible commodities centre and in its capacity as a government entity, Dubai Multi Commodities Centre (“DMCC”) is committed to supporting both domestic and international efforts and initiatives aimed at combating money laundering and the
financing of terrorism in addition to implementing such internal measure as may be deemed necessary.

2.2. The issuance of this Policy together with the implementation and operation of the procedures and controls therein, is a reflection of DMCC’s commitment in this regard.

2.3. DMCC is willing to co-operate with:

① Government agencies; and
② Recognized law enforcement agencies, domestic or foreign

As part of any effort in combating money laundering and/or the financing of terrorism.

3. POLICY CUSTODIAN

3.1. DMCC’s Management Team shall be the appointed custodian of this Policy and shall be ultimately responsible for the implementation and enforcement of the Policy.

3.2. The Management Team will be supported by the Compliance and Inspection Director who will provide expertise and assistance regarding the implementation and enforcement of the Policy.

4. PURPOSE AND RATIONALE

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

4.2. The rationale behind the Policy is unequivocally clear. DMCC will only accept those Members:

① Whose sources of funds can be reasonably established as legitimate; and
② Who do not pose any risk (actual or potential) to DMCC’s reputation.

4.3. In light of the foregoing, DMCC will not tolerate any involvement in illegal activities by its staff, Members or subsidiaries.

5. POLICY STATUS AND SCOPE

5.1. The provisions, procedures and controls detailed below are mandatory and shall apply to:

① DMCC staff; and
② DMCC’s Members and affiliates; and
③ DMCC’s subsidiary companies and divisions.

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

6. PROCEDURES AND CONTROLS (GENERAL)
6.1 This Policy contains, as an integral part to it, certain procedural checks and balances (collectively „Procedures and Controls“) so as to ensure the vigilant and effective operation of the Policy.

6.2 The Procedures & Controls are as follows:

- Identification, verification and know-your-customer („KYC“) measures
- Updating of KYC information
- Automated activity monitoring
- Reporting of suspicious activities
- Training and Awareness
- Record Keeping

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

7. PERIODICAL REVIEW

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

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

8.1. ID, VR, and KYC together form the first key step in the Procedures and Controls and is to be conducted prior to the granting of any DMCC membership to an applicant („Applicant“). It enables basic background information about the Applicant, their business, source of funds and their expected level of activity to be obtained and an initial decision undertaken.

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

8.3. Where Applicant is an Individual Person(s) Seeking To Form a DMCC Company

The ID, VR and KYC process must, in order to be valid, cover the following details regarding each individual Applicant:

- Applicant’s full name (as per NID or passport)
- Date and place of birth
- Nationality
- Physical address (residential and business / home country and UAE)
- Contact details
- Previous personal / business activities / occupation (type and volume)
- Anticipated type and volume of company’s activities
- Source of funds
- Bank reference and introductory letter
- Declaration re: Beneficial Ownership

1 „Beneficial Ownership“ is where a person has ultimate ownership or entitlement over funds.
The above list is a summary of the information required. A detailed checklist is attached in Appendix B.

8.4. Where Applicant is a Company Seeking To Form a DMCC Company

The ID, VR, and KYC process must, in order to be valid, cover the following details regarding the Applicant company:

① Incorporated name
② Shareholders² (in case applicant company being non publicly traded)
③ Beneficial owners³ (in case applicant company being non publicly traded)
④ Managers⁴
⑤ Signatories
⑥ Country of origin / UAE physical address (if applicable)
⑦ Contact details
⑧ Previous business activities (type and volume)
⑨ Anticipated type and volume of activities
⑩ Source of funds
⑪ Banking reference and introductory letter
⑫ Last two years audited financial statements
⑬ Details of external auditors

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

8.5. KYC Process

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

① Corporate KYC Checklist (please refer to Appendix A)
② Individual Shareholders / Managers KYC Checklist (Please refer to Appendix B)

8.5.2. The granting of DMCC membership to shell companies is strictly forbidden. For the purposes of this section 8.5, a ‘shell company’ shall mean an institution that has no physical presence in any country and which merely exists on paper.

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

² To include ‘active’ and ‘silent’ or ‘sleeping’ partners
³ In this particular context, ‘Beneficial Ownership’ means where a person owns 5% or more of the Applicant Company’s capital
⁴ That person having day-to-day control of the company if not a shareholder/partner
8.5.4. When conducting the KYC process, no reliance must be placed on third party information or ‘hearsay’ – ID, VR and KYC must all be carried out by DMCC itself. Example, if the Applicant is introduced to DMCC by a third party, DMCC is still under a clear obligation to perform the ID, VR and KYC procedures.

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

9. KYC INFORMATION UPDATING

9.1. Reasonable steps must be taken to ensure that ID, VR and KYC information is updated as and when required. As a minimum standard, KYC information must be updated every 2 (two) years.

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

10. AUTOMATED ACTIVITY MONITORING

10.1. Art 7 of Law No. 1 of 2003 gives DMCC the right to monitor, supervise and inspect the activities of its Members.

10.2. As such, the Members Activity Monitoring will be undertaken as follows:

   1) Reviewing the members’ annual Audited Financial Statements when they apply for Renewal of their Trade Licenses.

   2) Conducting Inspections on Members premises to ensure that their operations are conducted in accordance with UAE Regulatory System and DMCC Regulations.

11. REPORTING OF SUSPICIOUS ACTIVITIES

11.1 Art 15 of UAE Federal Law No. 4 of 2002 Regarding Criminalization of Money Laundering and Art 5.1 of the ESCA circular concerning procedures for AML place a clear obligation on all DMCC staff and Members to report any suspicious activities or information which may point to transactions, instructions, or arrangements with which DMCC is involved, being related to illegal activities. As money laundering and the financing of terrorism methods and techniques are always evolving, the Compliance and Inspection Department will issue regular circulars as what are to be considered as red flags for suspicious activities in both money laundering and financing of terrorism. These red flags will be the base on which the SARs should be filed by the different parties subject to this Policy. The red flags will also cover the attempted transactions.

---

5 DMCC Inspection Procedures Document
11.2 As such, it is the legal duty of management, staff and Members to report any suspicious activity or information (**) to the AMLSCU through the Compliance and Inspection Director. In doing so, it is important that:

① The reason for the suspicion is fully explained; and
② No mention of the suspicion is made to the Applicant, Member or Third party the subject of the suspicion (failure to observe this requirements may result in the divulging party being prosecuted for the offence of ‘tipping off’); and
③ Any additional information as may be requested by the Compliance and Inspection Director is duly provided.

11.3 All reports received under section 11.2 above will be treated in the strictest confidence.

11.4 The Compliance and Inspection Director will investigate the report and will decide on the information available together with any additional enquiries whether or not to file a Suspicious Activity Report with the Anti-Money Laundering and Suspicious Cases Unit of the UAE Central Bank.

11.5 Settlement transactions, whose cash value is equal to or exceeds forty thousand dirhams (= > AED 40,000) and considered as suspicious should be recorded by the DMCC staff and / or Members concerned and reported to the Compliance and Inspection Director.

12. TRAINING AND AWARENESS

12.1 Training shall be carried out at least once every two years for all relevant\(^6\) staff within DMCC, its subsidiaries and Members so to ensure they are aware of those AML and CFT regulations, controls and responsibilities which require their compliance and which form the basis of this Policy.

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

13. RECORD KEEPING

13.1 KYC Documentation
For the purposes of this section 13, „KYC Documentation“ shall refer to:

a) All Members’ documentation and/or correspondence regarding DMCC registration;
b) All Members’ documentation and/or correspondence regarding DMCC licensing;
c) Refused registration and licensing applications;
d) All documentation concerning a suspicious activity report concerning a Member together with any response/ follow up; and

\(^6\) Includes staff involved in activities from establishing the relationship, providing advice to members, and through all aspects of activities processing and monitoring
e) Records of AML/CFT training sessions attended by DMCC staff, Members, their dates, content and attendees.

13.2. Retention Periods

All documentation required under this Policy should be retained on site for a period of at least 5 years from the date of expiration/termination of a third party's DMCC Membership.

13.3. Investigations

Where a Member is the subject of an investigation of any kind then all documentation relating to the investigation must be retained for such time until the authority conducting the investigation (e.g. ESCA, Dubai Police, Interpol etc) informs DMCC otherwise in writing.

14. DMCC MANAGEMENT AND STAFF RESPONSIBILITIES

14.1 Scope of Responsibility

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

a) Undertake their due diligence role,

b) Ensure their and their team’s awareness of and compliance with ID, VR and KYC, record keeping and reporting; and

c) Undergo such ongoing AML/CFT training as DMCC deems necessary from time to time.

15. REFERENCES

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

- UAE Federal Law No. 4 of 2002 Regarding Criminalization of Money Laundering
- UAE Federal Law No. 1 of 2004 on Combating Terrorism Offence
- UAE Federal Law No. 8 of 2004 regarding the Financial Free Zones
- Federal Law No. 4 of 2000 Regarding The Emirates Securities and Commodities Authority and Market
- ESCA regulation concerning procedures for Anti-Money Laundering
- Rule No. 4 of 2002 for Organizing Operations at DMCC
- Rule No. 1 of 2003 Amending Certain Provisions of Rule No. (4) for DMCC
- DFSA RM08/2004
- FATF 40 AML and 9 CFT Recommendations
- IOSCO CIBO and AML Rules
- Basel Committee on Banking Supervision Recommendations
APPENDICES

Note:

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

① Registered and practicing lawyer; or
② Registered Notary Public; or
③ Chartered Accountant; or
④ Government ministry; or
⑤ Embassy or Consulate; and
⑥ UAE Ministry of Foreign Affairs
APPENDIX A – CORPORATE KYC CHECKLIST

The following information/documents must be collected and retained:

A1 Proof of legal existence of Applicant company:

- Trade License (if relevant in country of incorporation); and
- Certificate of Incorporation; and
- Memorandum and Articles of Association; and
- Board Resolution permitting DMCC application

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

A2 Proof of Applicant company’s physical address in country of origin and physical address within the UAE (when applicable):

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

A3 Contact details of Applicant Company:

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

A4 Names and addresses of all controlling individuals\(^7\) of the Applicant Company and its assets (verified as per Appendix B, Sections B1 and B3)

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

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

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

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

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

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

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

\(^7\) The expression „Controlling Individual” here means a shareholder, beneficial owner or a manager
A10 Details of Applicant company’s previous business including:

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

A11 Indication of the anticipated volume and type of activity to be conducted by the Applicant Company

A12 Understanding the source of funds originating from the Applicant Company

A13 First class bank reference whereby Applicant Company has been known to the issuing bank for at least two years

A14 Last two years audited Applicant company financial statements

A15 External Auditors name and address

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

For financial intermediaries only:

- Completed Sections A1 to A15 above; and
- Proof that the Financial Intermediary has been properly constituted, is supervised by a recognized authority and has good reputation; and
- Completed separate Application form
APPENDIX B – INDIVIDUAL SHAREHOLDER KYC CHECKLIST

The following information/documents must be collected and retained:

B1 Valid, original ID card (for UAE nationals) or passport clearly showing:
  □ Legal name (Change of Name Deed in the case of change of name);
  □ Date and place of birth; and
  □ Nationality

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

B2 Proof of country of origin and physical address therein of individual in the form of:
  □ Passport; or
  □ Home country National ID; or
  □ Home country Driving license

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

B3 Proof of individual’s physical address in the UAE in the form of:
  □ Original utility bill; or
  □ Copy of lease / purchase agreement

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

B4 Contact details of the individual:
  □ Telephone number(s);
  □ Fax number(s); and
  □ email address.

B5 Verification of contact details in B4 above via their testing by DMCC

B6 Previous personal and business profile of each individual shareholder, such profiles to include previous occupations and/or types of businesses operated
  □ Names and addresses of previous businesses or employers;
  □ Main products;
  □ Owners;
  □ Main customers and suppliers;
  □ Main activities geographical areas; and
  □ Volume of previous activities

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

B8 Understanding the source of funds (income, assets, net worth, etc) of each individual shareholder/manager
B9  First class bank reference whereby the individual has been known to the Issuing bank for at least two years
APPENDIX C – CORPORATE KYC UPDATING CHECKLIST

The following information/documents must be collected and retained:

C1 Same year proof of physical address of Member company in the form of:
   - Original utility bill; or
   - Copy of lease/purchase agreement

C2 Recent contact details of Member Company:
   - Office telephone number(s);
   - Office fax number(s);
   - Office email address; and
   - Website address

C3 Names and address of all new (since registration date or last update) beneficial owners and controlling individuals (Managers) of the Member Company and its assets (verified as per Appendix B, Sections B1 and B3).

C4 Declaration by each Member company authorized signatory that the latest beneficial owners mentioned in C3 above are the sole beneficial owners of the Member Company.

C5 Description of Member company’s activities (types and volume) for the last two years

C6 Member company’s financial statements for the last two years audited by one of the DMCC approved external auditors

C7 External auditors name and address
APPENDIX D – INDIVIDUAL SHAREHOLDER AND / OR MANAGER
KYC UPDATING CHECKLIST

The following information/documents must be collected and retained:

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

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

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

D2 Same year proof of physical address of individual:

□ Original utility bill; or
□ Copy of lease agreement; or
□ Copy of deed agreement

D3 Latest contact details of the individual:

□ Telephone number(s);
□ Fax number(s); and
□ Email address
APPENDIX E – PRACTICAL ISSUES CONCERNING TRAINING AND AWARENESS (SECTION 12)

E1 Any training provided under section 12 must include:

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

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

- Handbooks
- Awareness messages
- Courses (internal and external)
- Induction programs
APPENDIX F – PRACTICAL ISSUES CONCERNING RECORD KEEPING (SECTION 13)

F1 Storage Location

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

Suitable external locations may be:

- A secure area (e.g. warehouse, office) owned and/or operated by DMCC; or
- A secure area owned and/or operated by a reputable third party provider such as Infofort.

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

F2 Use of Other Storage Media

As an additional safeguard, the Company may elect to scan images of original documents onto CD-Rom format. CD-Rom’s should be stored in a secure environment suitable for the long term storage of electronic/digital media.

F3 Data Retrieval/Accessibility

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

As such, stored KYC Documentation should be indexed by reference to:-

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