FIX TRADING COMMUNITY

DOCUMENT RETENTION POLICY

1. POLICY OVERVIEW

1.1 This Document Retention Policy ("**Policy**") defines the minimum requirements for the maintenance, storage, retrieval, retention and destruction of the documents and records of FIX Protocol Limited ("**FIX**"), the FIX Trading Community (the "**Community**") and its members.

1.2 FIX is committed to effective records management to comply with applicable laws and meet the information retention and retrieval needs of its operations. This Policy describes FIX's document management procedures and should be read along with all other relevant FIX policies.

1.3 Specifically with regard to the antitrust / competition compliance policies of FIX, we draw your attention to the section entitled "legal exception" (at Section 7). It is imperative that in the event of any regulatory investigation or site inspection by national, federal or state officials that all documentary destruction processes are immediately suspended. Members of the community must also refrain from informing each other (or anyone outside their own organisation) that an inspection is taking place.

1.4 FIX expects all employees to understand and comply fully with this Policy. No policy, however, can cover every document management issue or situation that may arise. Any questions regarding document retention and destruction issues not covered by this Policy should be addressed to the Data Privacy Officer (the "**DPO**") or Legal Team in your jurisdiction.

1.5 In the context of FIX, the DPO is Ms Courtney McGuinn.

1.6 FIX realises that members of the Community outside of its own corporate group will have their own policies. FIX advises members to consult with their own internal document retention policies with regard to the way in which they administer their organisation's documents and records. They may also wish to consult with their own DPO and/or document management or Legal Team in connection with issues arising from this policy document.

1.7 FIX would, however, strongly expect and recommend that the data retention policies of its members would as a minimum respect the principles set out in this document, particularly those set out at paragraphs 1.3 and 7.

2. PROCEDURE

2.1 FIX requires that certain types of records be retained for specified periods in compliance with applicable laws. These records must be managed in accordance with the procedures outlined in this document and the Record Retention Schedule in section 10 of this Policy (the Retention Schedule) notwithstanding the applicable law in the jurisdictions where a FIX entity is situated.

2.2 In all circumstances however, the Legal Exception overrides the time periods in the attached Retention Schedule. Further information on what to do in such circumstances is provided below under Legal Exception – Modification of Document Retention Procedures.

2.3 In general, FIX's policy is to maintain records for the periods stated in the Retention Schedule unless the Legal Exception applies.

2.4 FIX may choose to comply with legal requirements by storing certain records electronically. This will not, however, change the required retention period.

3. DEFINITIONS

3.1 "**Records**" means all and any records containing business and personal data and information, including paper documents, including but not limited to final versions, drafts, correspondence, handwritten notes, and diary entries, as well as video and audio tapes and all computer files, e-mail, and other documents or data in electronic form on hard drives, servers, disks, back-up tapes, hand-held devices, or any other media or devices.

3.2 "**Register**" has the meaning given at para 8.1.4.

3.3 "**Legal Exception**" means FIX records which are or may be relevant to actual or potential litigation, dispute or government investigation, must be preserved under the control of the Legal Team in the relevant jurisdiction.

3.4 "**Legal Team"** means a team of in-house counsel or advisers within an organisation responsible for advising on legal matters affecting the organisation and its business dealings.

4. RECORDS CONTAINING PERSONAL DATA

4.1 Records containing personal data must be:

4.1.1 stored appropriately having regard to the sensitivity and confidentiality of the material recorded;

4.1.2 retrievable and easily traced;

4.1.3 retained for only as long as necessary; and

4.1.4 disposed of appropriately and to prevent records falling into the hands of unauthorised personnel.

4.2 Any data file or record which contains personal data of any form should be considered as confidential in nature.

5. DUPLICATES

Unless the Legal Exception applies, multiple and duplicate copies of reports, filings, and other FIX records, inter-employee correspondence and memoranda, and data need not be retained, provided that any person disposing of such material has first confirmed to his or her reasonable satisfaction that the FIX employee routinely charged with maintaining such records is doing so in accordance with this Policy. Any questions should be directed to the DPO.

6. STORAGE OF RECORDS

6.1 All data and records should be stored as securely as possible in order to avoid potential misuse or loss. All data and records will be stored in the most convenient and appropriate location having regard to the period of retention required and the frequency with which access will be made to the record.

6.2 The degree of security required for file storage will reflect the sensitivity and confidential nature of any material recorded. HR records will be kept in a secure cabinet accessed only by authorised personnel.

6.3 Data and records should be stored in the most appropriate place for their purpose.

7. LEGAL EXCEPTION – MODIFICATION OF DOCUMENT RETENTION PROCEDURES

7.1 If:

7.1.1 FIX receives notice that it or a director, officer, or employee has been made a party to litigation or an investigation by a governmental department or agency,

7.1.2 FIX reasonably anticipates that it, or a director, officer, or employee, may be party to litigation or that there is potential for a governmental investigation or proceeding related to company activities, or

7.1.3 FIX or an affiliate, or a director, officer, or employee, receives notice of a subpoena for documents**,**

- FIX will implement a plan to preserve relevant records.

7.2 The Legal Team in the relevant jurisdiction should be consulted in connection with any decision on whether documents should be preserved in response to a legal matter. In the event you are required to suspend normal document retention procedures for legal reasons, you will receive a "Litigation Hold Notice" or other written notice from the Legal Team.

7.3 If any employee learns of information suggesting that there is any actual or potential litigation, investigation, or other proceeding against or involving FIX or a director, officer, or employee, the employee must immediately notify the Legal Team in his/her jurisdiction. Employees who assist in gathering information at counsel's direction should work with counsel to ensure that their efforts are appropriately documented.

7.4 No director, officer or employee of FIX shall destroy any document relevant to the subject matter of the investigation or litigation without specific written authorisation from the Legal Team.

7.5 Knowing destruction by any FIX employee of documents related to a pending or anticipated civil or criminal proceeding or investigation may be grounds for disciplinary action up to and including possible termination of employment. Further, such conduct may subject the employee to civil and criminal penalties.

7.6 The Legal Team in each jurisdiction shall inform all personnel who have been instructed for legal reasons to suspend FIX's usual document destruction procedures when it is appropriate to resume those usual procedures.

7.7 Any questions regarding retention of documents, including whether a legal matter requires suspension of FIX's usual document destruction procedures or whether specific documents are relevant to a legal matter, should be directed to the DPO.

8. DESTRUCTION AND DISPOSAL

8.1 Regular disposal

8.1.1 All information of a confidential nature whether on paper, card or electronic media must be securely destroyed when it is no longer required. FIX has waste bins for confidential material situated throughout its offices in various jurisdictions.

8.1.2 All office paper should be shredded if the content is in any way sensitive.

8.1.3. If you dispose of waste by using the shredder, ensure that it is used safely in accordance with its operating instructions, and that waste is shredded in such a way that it cannot be put back together again.

8.1.4 When you dispose of records or data files which are due for disposal as per section 10.4 of the Retention Schedule, a note should be made of the disposal in the register of record disposals (the "**Register**").

8.2 One-off destruction

If there is a substantial quantity of records due for destruction (i.e. past their retention period) a one-off destruction is potentially appropriate (for example, when a business unit or employee is relocated); the following procedures apply:

8.2.1 Clearly document what records are being considered for possible destruction;

8.2.2 Review a representative sample to determine content and the appropriateness of destruction;

8.2.3 Classify the records into groups where possible;

8.2.4 Verify with the Legal Team in his/her jurisdiction that none of the records should be retained for purposes of any current or anticipated litigation or investigation. If the Legal Team identifies documents as having to be retained for any such legal purpose, those documents shall be retained in strict accordance with counsel's instructions;

8.2.5 Prepare a description of each group of records to be destroyed and circulate the description to appropriate department managers to get approval;

8.2.6 Once all necessary approvals are obtained, use a destruction method that ensures confidentiality; and

8.2.7 Document the destruction including date, description of groups destroyed, method of destruction, and individuals involved, in the Register.

8.3 The following general principles should be considered when considering the disposal of records:

8.3.1 Is the record significant in terms of development or policy change or HR (e.g. minutes of meetings, contracts, employee records)

8.3.2 Does the record relate to a transaction which set, or is likely to set, a precedent?

Example: versions of contracts

8.3.3 Does the record contain data which would be useful for retrospective comparisons?

Example: company P & L records

8.3.4 Does the record contain systematically recorded data which is not easily available elsewhere?

Example: management agreements records and statistics.

8.3.5 Does the record contain information gathered from outside FIX?

Example: statistics from competitors

8.3.6 Is the record likely to be useful as legal evidence in the future?

Example: papers relating to disputes or HR Issues

8.4 All other paper can be disposed of in the boxes or bins provided in offices for disposal of non-confidential and non-sensitive paper waste.

8.5 The procedure for the destruction of confidential or sensitive waste on electronic media such as tape, disk, cassette/cartridge, hard drives, CD-Rom, DVD and ZIP drive is as follows: media that are being destroyed because they are showing signs of damage or are obsolete should be physically destroyed by being cut into pieces or by other means prior to disposal.

8.6 Where disks, tapes, DVD or CD ROM are being used to supply data to third parties they should, at the very least, be reformatted before the files are saved on to it. The process of saving files to the disk may overwrite areas of the disk previously used, but this is no guarantee of preventing retrieval of previously stored files. The most effective way to ensure that media are cleaned of all previous data is to use a utility package to perform a "secure wipe".

9. DEPARTMENT MANAGERS

9.1 Department managers shall be responsible for:

9.1.1 Identifying the specific Records as listed in the Retention Schedule;

9.1.2 Identifying Records required to meet business regulations;

9.1.3 Establishing methods for orderly processing, filing, identifying, labelling, storing and maintaining Records;

9.1.4 Implementing appropriate security measures to prevent unauthorised changes, removal or access to Records;

9.1.5 Destroying Records in a confidential manner when the applicable Record retention period expires; and

9.1.6 Ensuring that staff keep the Register up-to-date.

10. RECORD RETENTION SCHEDULE

10.1 Notwithstanding the applicable law in the jurisdictions where a FIX entity is situated, the following retention period in section 10.4 applies.

10.2 Before sending any records to storage, the responsible employee should prepare an itemised list of the files contained in each box. Each business unit should store such lists in a centralised location to facilitate retrieval efforts should they become necessary.

10.3 This Policy applies equally to electronic and paper records. The period of retention only commences when the record is closed. Records retention periods reflect the minimum length of time that a Record must be maintained and accessible.

10.4 The following table defines the Record Retention Schedule for most common Records, unless there is more specific schedule in any of the affiliates:

Department	Description of Data	Retention Period or Recommendation
Finance	Accounting Records – e.g, income and expense records, records of assets and liabilities of the company, statements of stock held by the company, statements of all goods sold and purchased, etc	10 years
Finance	Company Tax Returns	6 years
Customer Service and Sales	Sales correspondence, invoices and documents and contracts	6 years after the end of the relationship
Legal	Company incorporation documents, appointments of directors and/or shareholders	Retain for the life of the company and 10 years after dissolution of the company
Legal	Record of directors' meetings, shareholders' resolutions and minutes of general meetings	10 years from the date of the meeting/decision
Legal	Litigation files	7 years
HR/Legal	Employment matters - termination of employment, grievances, etc.	While the employment continues and 7 years after the employment ceases
HR/Finance	Salary-related data	While the employment continues and 7 years after the employment ceases
HR	Recruitment data of unsuccessful candidates	2 years after notifying unsuccessful candidates
Marketing	Advertising and promotional materials	5 years
Email correspondence	Emails sent and received between members in relation to FIX Protocol and its	Retain for the lifetime of the company

	activities.	
Deliverables from working groups	Documents produced from collaboration between members including for example best practices and other documentation for the wider industry.	Retain for the lifetime of the company