MOTILAL OSWAL SECURITIES LIMITED

PRESERVATION OF DOCUMENTS AND ARCHIVAL POLICY

Details of Amendments to the Policy				
Policy Change effective Date	**Clause No.**	**Particulars of the Change**	**Board Approval Date**	**Version of Policy**

I. SCOPE OF THE POLICY

A. This policy is prepared in accordance with the requirements of the provisions of Regulation 9 and Regulation 30 (8) of the SEBI (Listing Obligation and Disclosure Requirements) Regulation, 2015 **("Listing Regulations")**. The Board of Directors **("Board")** of **Motilal Oswal Securities Limited ("Company")** has adopted this policy at its meeting held on 30th January, 2017, to establish the authorization for identifying, creating, maintaining, managing, organizing, administering, retaining, storing, protecting and disposing-off the company's records, documents and information.
B. This policy is also prepared to recognize and ensure the preservation and availability of the official records of the Company for legal, administrative and historical purposes.

II. OBJECTIVE OF THE POLICY

A. The twofold objective of this policy is to provide guidelines for the employees for the preservation, retention, and destruction of the documents of the Company's records and to create the right environment for the procedure and methodology of archiving the documents of the Company, to ensure accountability in a manner which shall provide for prompt retrieval of information while reducing storage requirements for inactive and outdated documents.
B. This Policy may be amended at any time by the Board of Directors of the Company and is subject to further guidance from SEBI or amendments to or re-enactment of Regulations.

III. RELEVANT REGULATIONS

A. Chapter III, Regulation 9 of the Listing Regulations prescribes the Company to have a policy for the preservation of documents which has to be classified into further two categories.

"*Regulation 9 - Preservation of documents.*

9. The listed entity shall have a policy for preservation of documents, approved by its board of directors, classifying them in at least two categories as follows-
(a) documents whose preservation shall be permanent in nature ;
(b) documents with preservation period of not less than eight years after completion of the relevant transactions:

Provided that the listed entity may keep documents specified in clauses (a) and (b) in electronic mode.

B. Chapter III, Regulation 10(8) of the Listing Regulations prescribes the Company to have an archival policy which shall ensure the preservation of information which the Company discloses to stock exchanges.

"Regulation 30- Disclosure of events or information.

(8) The listed entity shall disclose on its website all such events or information which has been disclosed to stock exchange(s) under this regulation , and such disclosures shall be hosted on the website of the listed entity for a minimum period of five years and thereafter as per the archival policy of the listed entity, as disclosed on its website"

IV. POLICY STATEMENT

A. PRESERVATION:

a. The Company will generate, use, maintain, store, and destroy records in accordance with the requirements of applicable laws and other applicable standards.

b. Records are organized and stored by authorized records custodian(s) to ensure that they are easily accessed and retrieved in a timely manner.

c. Records are stored in space (physical and electronic) that is appropriate for their classification.

d. Records maintained in the company facilities shall be preserved in a manner consistent with the storage requirements specified by the Compliance Officer (or such other person from the management as may be deemed appropriate).

e. In order to simplify the processes by which company records are placed in long-term storage facilities, the management may identify those storage locations outside of company facilities that are approved for offsite storage for preservation purpose.

f. All records generated and received by the company are the property of company, regardless of how or who created them or where they are maintained. No company employee, by virtue of his or her position, has any personal or property right to such records even though s(he) may have developed or compiled them, including but not limited to company records created on home or non- company computer equipment used by the employees for work related purposes.

g. The unauthorized copying, transfer, dissemination, destruction, removal or use of company records is prohibited.

Table A:

Sr. No.	Preservation Permanent in Nature	Preservation period of not less than eight years after completion of transactions
1	Material Contracts	Accounts & Finance
2	Mergers & Acquisition documents	Corporate (Secretarial) Records
2	Legal files and papers	Regulatory
3	Manufacturing	Miscellaneous
4	Information Technology (E-Mail)	Personnel
5	Pension Documents And The Supporting Employee Data	Quality Control And Inspection
6	Procurement Material Control	Research And Development
7	Safety And Environmental Documents	Sales And Marketing
8	Intellectual Property Rights (IPR)	Tax Records
9	--	Traffic And Transportation

h. A back up of all the official records, information and the data of the Company's personnel having their designation of Senior VP and above shall be taken on a regular basis.

i. A back up of all the records, information and the data of all the respective departments shall be taken on a weekly basis.

j. Records under the two head's as classified above may keep and maintain them in the electronic mode.

ESI (electronic record) is to be maintained in the company facilities in a manner consistent with the SOP concluded by the Information Technology department of the Company. Any offsite storage facilities are to be in secure locations that safeguard the records from (i) virus or other malicious, destructive or corrupting code, program or macro in the process; (ii) sabotage and computer hacking unauthorized access to computer data and storage devices; and (iii) system crashes etc.

B. RETENTION:

a. Regardless of minimum retention periods, all records shall be kept until audits (if any) are completed and any proposed corrective action has been implemented. Records are created and maintained to provide complete and accurate evidence of company's business.

b. Records that have satisfied their required period of retention and are no longer required shall be disposed in an appropriate manner consistent with this Policy.

c. All company personnel who have access to or use records are responsible for ensuring that records are generated, used, maintained, stored, retained and destroyed in accordance with the Policy.

d. Keeping in view the limitation of space and the fact that records keep on increasing with passage of time, it is necessary to provide a system for retaining only the relevant records which are most likely to be required. The company personnel shall refer to the above Table A above.

e. Internal audit team may perform operational audits of company records and information systems.

f. This Policy supersedes any conflicting practices, procedure or policy.

g. Unless the context otherwise requires, most correspondence and internal memoranda should be retained for the same period as the document they pertain to or support. For instance, a letter pertaining to a particular contract would be retained even after such contract expires or is terminated as long as such contract/agreement contains retentionprovision (e.g. Obligation of the parties shall continue 10 years after expiration).

h. Confidential records must be securely maintained, controlled and protected to prevent unauthorized access or disclosure. Confidential & proprietary records may be shared internally as appropriate to the conduct of business, and with third parties only after it has been properly marked or identified. Any records labeled as "Privileged & Confidential" or "Confidential" or "Confidential & Proprietary" shall be separately maintained by the respective user department, or otherwise adequately secured under the supervision of the Compliance Officer or the respective Controlling Authority, and not destroyed or disclosed in any manner except under the direction of the Compliance Officer or such Controlling Authority.

a. Vital Records are to be duplicated onto appropriate media and the duplicate records stored in the designated storage facilities, for reconstructive use in the event of a natural or man-made disaster. In the absence of a legal hold, only one copy (generally

the original, fully executed version of the record where available) of each record must be retained. When establishing a system or procedure for scanning /microfilming, it would be advisable to retain hard copy for a specified amount of time until satisfaction with the scanning system can be assured.

b. Records that are retained in the ordinary course of company's business information back-up procedures pursuant to its electronic record retention and destruction practices should be (a) maintained only oncentralized storage devices (and not on personal computers or devices),(b) not accessible by any of Company personnel (other than company information technology department), and (c) are not otherwise accessedsubsequently except with the written consent of the Compliance Officer or the respective Controlling Authority.

c. Except as otherwise expressly provided herein, records are maintained only for as long as administratively needed. Records may be discarded when the need for retention has ended and there is no legal or governmental process pending with regard to such Records.

d. Drafts of documents may be retained until completion of the final document. After the document has been issued in its final form, the drafts may be discarded and only the final version retained. Personal notes such as notes of meeting should not be retained after they are no longer needed.

e. **Records Center** – Physical records are to be maintained in the company facilities in a manner consistent with the storage requirement specified by the Compliance Officer (or such other person from the management as may be deemed appropriate). Any offsite storage facilities are to be in secure locations that safeguard the records from (i) ordinary hazards, such as fire, water, mildew, rodents and insects; (ii) man-made hazards, such as theft, accidental loss, sabotage, and commercial espionage; (iii) disasters, such as fire, flood, earthquakes, hurricanes, wind, and explosions; and unauthorized use, disclosure and destruction etc.

C. DESTRUCTION

a. In the absence of an investigation or litigation, (i) transitory records may be destroyed or disposed of upon completion of their use and (ii) Records may be destroyed or disposed of after the expiration of their retention period as set forth in the Schedule unless the Compliance Officer (or such other person from the management as may be deemed appropriate) or the Controlling Authority authorize an exception.

b. Records that cannot be destroyed include records of matters currently subject to governmental audit or in litigation, or records with a permanent retention. In the event of a lawsuit or government investigation, the applicable records that are not permanent cannot be destroyed until the lawsuit or investigation has been finalized. Once the litigation/investigation has been finalized, the records may be destroyed in accordance with this Policy.

c. At the time of destruction, the Company should record the actual date of destruction on the '**Records Destruction Authorization Form'** and attach any supporting documentation, such as a **'Certificate of Destruction'**. Please note that if the Company contracts with a commercial vendor, the vendor should provide a **'Certificate of Destruction'** attesting to the actual destruction of the records and specifying the types and quantities of records destroyed the method of destruction, the destruction date, and agreeing to maintain the confidentiality of the documents it destroys.

d. Respective Controlling Authority, who is authorised destruction ofthe Records, shall quarterly send summary report to the ComplianceOfficer including linked Records Destruction Authorisation form,Certificate of Destruction etc. The Reports shall certify and document Controlling Authority's compliance with this Policy.

e. Destruction of Records refers to either destruction of Records or transfer of records to the custody of another entity. Records may not be destroyed or transferred until the Compliance Officer (or such other person from the management as may be deemed appropriate) or the Controlling Authority has returned a signed 'Records Destruction Authorization form' to the requester. If a record does not appear on a Records Retention Schedule, it does not mean that the Company may dispose of the Record without permission from the Compliance Officer (or such other person from the management as may be deemed appropriate) or the Controlling Authority.

f. Destruction Authorisation- The destruction of company records should be authorized by the Compliance Officer (or such other person from the management as may be deemed appropriate) or by the ControllingAuthority.

V. IMPLEMENTATION AND MONITORING

Employees: responsible for knowing and following the Policy and procedures for Records created or received by the employee while conducting Company business.

Compliance Officer: Compliance Officer as defined under the SEBI (Prohibition of Insider Trading) Regulations, 2015 shall be administrator in charge of this Policy. His/her responsibilities are supervising the retention and destruction of Records and recording the actions taken to retain and/or destroy them. The Compliance Officer may modify and review this Policy to complywith Applicable Laws and organizational policies. Compliance Officer may approve and document exceptions to this Policy on an "as needed basis".

Functional Head/ Controlling Authority: Except as otherwise expressly provided herein, Functional Head/ Controlling Authority is responsible for assigning and ensuring the training and active participation of thedepartmental employee(s); ensuring departmental compliance with this Policy, procedures, and principles; and,

maintaining departmental records until their final disposition. Functional Head/Controlling Authority may delegate their authority/responsibility to appropriate individualswithin their departments, but remains responsible under this Policy. Any such delegation must be in accordance with the 'Delegation of Authority' matrix available with the legal department.

Records Custodian: authorized employee or third party who is responsible for managing a Record Center. This includes the maintenance, security, protection, access, and routine disposal of Company Records.

VI. CHANGE IN POLICY

The Authorised KMP's after approval of the Board may amend or modify this Policy in whole or in part, at any time.

****