

RISHIROOP LIMITED

DOCUMENT PRESERVATION, DESTRUCTION & ARCHIVAL POLICY

1. Policy and Purposes

This Policy relating to preservation, destruction, and archival of documents of Rishiroop Limited (the 'Organization/Company') with respect to the retention, destruction, and archival of documents and other records, both in hard copy and electronic media (referred to as 'documents' in this policy) has been framed as per the requirement of Reg. 9 and Reg. 30(8) of SEBI (Listing Obligation and Disclosure Requirement) Regulations, 2015.

Purposes of the Policy include :

- (a) retention and maintenance of documents necessary for the proper functioning of the organization as well as to comply with applicable legal requirements;
- (b) destruction of documents which no longer need to be retained;
- (c) archival of documents; and
- (c) guidance for the Board of Directors, officers, staff with respect to their responsibilities concerning document retention and destruction.

2. Administration

2.1 Responsibilities of the Administrator. The Company's Chief Financial Officer (CFO) shall be the administrator ("Administrator") in charge of the administration of this Policy. The Administrator's responsibilities shall include supervising and coordinating the retention, destruction and archival of documents pursuant to this Policy and particularly the **Document Retention Schedule** mentioned in point 6. below. The Administrator shall also be responsible for documenting the actions taken to maintain and/or destroy organization documents and retaining such documentation.

2.2 Responsibilities of Other Persons. This Policy also relates to the responsibilities of board members and staff with respect to maintaining and documenting the storage and destruction of the organization's documents. The Administrator shall report to the Board of Directors. The organization's staff shall be familiar with this Policy which shall be uploaded on the website of the Company. They shall act in accordance with the Policy, and assist the Administrator, as requested, in implementing it.

3. Suspension of Document Destruction; Compliance. If the Administrator becomes aware that litigation, a governmental audit or a government investigation has been instituted, or is reasonably anticipated or contemplated, the Administrator shall immediately order a halt to all document destruction under this Policy, communicating the order to all in writing. Failure to comply with this Policy, including, particularly, disobeying any destruction halt order, could result in disciplinary action including possible termination.

4. Electronic Documents; Document Integrity. Documents in electronic format shall be maintained just as hard copy or paper documents are, in accordance with the Document Retention Schedule. Due to the fact that the integrity of electronic documents, whether with respect to the ease of alteration or deletion, or otherwise, may come into question, the Administrator shall attempt to establish standards for document integrity, including guidelines for handling electronic files, backup procedures, archiving of documents.

5. Emergency Planning. Documents shall be stored in a safe and accessible manner. Documents which are necessary for the continued operation of the organization in the case of an emergency shall be regularly duplicated or backed up and maintained in an off-site location. The Administrator shall develop reasonable procedures for document retention in the case of an emergency.

6. Document Retention Schedule.

Document Type

Retention Period

Accounting and Finance

Documents to be retained for the minimum period prescribed below or as prescribed by Statute/Rules which are in force, and modified from time to time :

Books of Accounts	8 years
Annual Financial Statements and Audit Reports	Permanent
Bank Statements, Reconciliations, Deposit Slips, NEFT/RTGS advice	8 years
Employee/Business Expense Reports/Documents	8 years
Sales/Purchase Invoices	8 years
Import/Export Documents	8 years
IncomeTax Returns/Orders/Intimations/Appeals etc.	Permanent
PAN Card/ PAN Allotment Letter	Permanent
Records relating to Excise, Customs, Service tax, FEMA	As per relevant statute

Corporate

Memorandum & Articles of Association	Permanent
Minute Books, including Board & Committee Minutes	Permanent
Statutory Registers	Permanent
Annual Reports	Permanent
Other Corporate Filings (ROC Forms, Challans etc.)	Permanent
Licenses and Permits	Permanent

Correspondence and Internal Memoranda

Hard copy correspondence and internal memoranda relating to a particular document otherwise addressed in this Schedule should be retained for the same period as the document to which they relate.

Hard copy correspondence and internal memoranda relating to routine matters with no lasting significance - Two years

Correspondence and internal memoranda important to the organization or having lasting significance - Permanent

Electronic Mail (E-mail) to or from the organization

Electronic mail (e-mails) relating to a particular document otherwise addressed in this Schedule should be retained for the same period as the document to which they relate, but may be retained in hard copy form with the document to which they relate.

E-mails not included in the above category - 12 months

Electronically Stored Documents

Electronically stored documents (e.g., in pdf, text or other electronic format) comprising or relating to a particular document otherwise addressed in this Schedule should be retained for the same period as the document which they comprise or to which they relate, but may be retained in hard copy form (unless the electronic aspect is of significance).

Electronically stored documents considered important to the organization or of lasting significance should be printed and stored.

Electronically stored documents not included in either of the above categories - Two years

Employment, Personnel and Pension

Personnel Records	8 years after employment ends
Employee contracts	8 years after termination
Retirement and pension records	8 years

Insurance

Property and General Liability Insurance Policies	8 years
Insurance Claims Records	8 years

Legal and Contracts

Contracts, related correspondence and other supportings	10 yrs after termination
Legal correspondence	Permanent

Management and Miscellaneous

Strategic Plans	8 years after expiration
Policies and Procedures Manual	Current version with revision history

Property – Real, Personal and Intellectual

Property deeds and purchase/sale agreements	Permanent
Lease Deeds	Permanent
Trademarks, Copyrights and Patents	Permanent

Where the preservation period of Documents is not included in the above identified categories, such period shall be determined by the application of the general guidelines affecting Document preservation identified in this Policy, as well as any other pertinent factors.

Any document not included above, should be maintained for a minimum period legally required and in other cases as determined by the respective head of the department in writing.

7.0 ACCESSIBILITY AND RETRIEVAL OF RECORDS

7.1 Retention of Physical records

Preserved records shall be kept confidentially, securely with access control and with ease of retrieval, whether in-house or externally. Measures should be taken for physical security of the records maintained like selection of area of record room, firefighting device, access control, etc.

7.2 Retention of Electronic Records

Wherever allowed/required by any law/statute, records may be maintained in electronic form.

In case of switch-over to another electronic system, it should be ensured that all the records in the old electronic system should be migrated to new electronic system and all old records are accessible in the new system.

8.0 DESTRUCTION & ARCHIVAL OF DOCUMENTS

All information generated in the course of the Company's business activities that is not required to be retained must be safely destroyed or discarded as soon as practicable, but in any event within 180 days of the completion of the project/assignment/contract.

8.1 Physical:

Destruction : The Documents should be destroyed at the end of the preservation period specified under Clause 6 of this Policy only after the written approval of the Administrator. The destruction should be carried out in a way that preserves the confidentiality of any information they contain, if so required. A record should be kept about the Documents that have been destroyed.

Archival : Records which are required to be maintained for certain period of time or permanently shall be added to the archive when it no longer has a business need. Files or items when added to the archive will be recorded on a database that shall be maintained, and retrieving the records from the archive must be for valid business reasons and with the approval of the Administrator. Retrieval from archive to be also recorded on database.

Documents should be shredded through a paper shredding machine, and not sold as scrap.

8.2 Electronic:

Destruction : Electronic information, including e-mails that are no longer required to be retained, must be purged only after the written approval of the Administrator using appropriate techniques which ensure that the data cannot be reconstructed from the storage media on which it resided. Records stored on magnetic media must be destroyed by reformatting at least once. The backup copies of the records must also be destroyed.

Archival : Electronic records no longer having business need but required to be stored for a certain period or permanently to be added to electronic archive. Database of such records to be maintained, and retrieval to be documented.

Electronic Data Security / Back up Process :

- All users data to be stored in data server
- Official data not stored in users local disk
- Druva Phoenix Backup system employed for server data backup
- Druva Phoenix protected by 256 bit AES (Advanced Encryption Standard) encryption and 256 bit SSL encryption security
- Data backup from data server to backup server every 2 hours on incremental basis
- Backup restoration copy taken on external HDD once in 3 months, and kept at a separate/remote location
- Restoration of data from backup server once in a year
- Druva Phoenix Cloud backup is under consideration.

9.0 REVIEW AND AMENDMENT

The Policy shall be reviewed as and when required to ensure that it meets the objectives of the Statutory Provisions and remains effective.

This Policy shall be reviewed periodically and may be amended by the Board of Directors of the Company, as may be deemed necessary.

10.0 INTERPRETATION

In case of any conflict between the provisions of this Policy and of Statutory Provisions, the Statutory Provisions shall prevail over this Policy. Any subsequent amendment/ modification in the Statutory Provisions shall automatically apply to this Policy.

In case of any clarification required with respect to this Policy, kindly contact the Company Secretary of the Company.
