

Jenburkt Pharmaceuticals Limited

**POLICY ON PRESERVATION, ARCHIVES
MANAGEMENT AND DESTROYING OF
DOCUMENTS**



POLICY ON PRESERVATION, ARCHIVES MANAGEMENT AND DESTROYING OF DOCUMENTS

1. Purpose:

The purpose of this policy is to establish the framework needed for effective records management at Jenburkt. This policy is for setting standards for classifying, managing and storing of Jenburkt's records.

In order to efficiently conduct its business, the storage, retrieval and management of these information reserves is a significant issue.

This policy is concerned with all aspects of Jenburkt's record keeping and seeks to ensure that the Jenburkt's business is adequately documented through the creation of records that are then managed in accordance with best practice along with regulatory requirements.

2. Definitions:

Archive: The whole body of records of continuing value of the Company. Those records that are appraised as having continuing value. It covers preserving documents of all of Jenburkt's functions, processes, activities and transactions and about its employees.

Disposal or destruction: These include the deletion or destruction of records in or from record preserving systems. They may also include the migration or transmission of records between record preserving systems, and the transfer of custody or ownership of records.

Electronic records : Records communicated and maintained by means of electronic equipment.

Information systems: Collections of hardware, software, supplies, policies, procedures and people, which store, process and provide access to information.

Record preserving : Making and maintaining complete, accurate and reliable evidence of business transactions in the form of recorded information.

Records or documents: Shall include physical and electronic records, reports, statements, documents, filings, certificates, licenses, permissions, any other information as required, information in any form including data in computer systems, created or retrieved and maintained by Jenburkt or its employees or by the person in the conduct of affairs of the Company.

3. Scope:

This policy is applicable to all the employees at all the locations of Jenburkt.



To create, store, maintain and preserve the records of the Company, the employees should be aware that electronic documents have the same status as paper documents. Both electronic and paper documents are subject to the same degree of confidentiality and care. Therefore electronic records must be managed as physical documents, as part of a comprehensive record preservation system.

4. Requirement:

4.1 Jenburkt does need such a sound policy to preserve documents, the quantity of which increases with its growth. Preserving and retrieval of document within Company is a challenging task.

4.2 Further, Securities and Exchange Board of India vide its regulation viz. Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015 have expressly stated that all the listed entity shall have a policy for preservation of certain documents and their time bound archival which are required under applicable laws. It further states to preserve the said documents in two categories: (a) documents to be kept permanently and (b) documents to be kept for a period less than eight years.

4.3 Destruction of documents which are of no use and which are not required to be preserved / archived statutorily.

5. Roles And Responsibilities Of Administrator(s):

Overall responsibility for records management rests with the Administrative Department under the direct supervision of the Chairman and Managing Director / Whole Time Director and CFO. They have ultimate responsibility to ensure that the Company complies with the requirements under this Policy.

Management-level staff and other staff of employees are responsible for implementing and maintaining the documents record keeping practices within their respective functional division.

Managers must ensure that documents are created, maintained and stored in accordance with the standards outlined in this policy, and that no records are destroyed except as authorised by the above mentioned officials.

6. Preservation Of Documents:

6.1 Storage

Records should be stored in conditions that are clean and secure, with low risk of damage from fire, water, dampness, mould, insects and rodents. They should also be kept away from direct sunlight and other sources of light and heat. The storage area should be well ventilated and ideally maintained at a stable temperature and humidity. Specialised storage conditions and handling process if required should be made available. Irrespective of format, documents of continuing value require higher quality storage and handling to preserve them for as long as that value exists. These



documents shall be stored in two categories: (a) documents to be kept permanently and (b) documents to be kept for a period less than eight years.

6.2 Amendment / revision:

Earlier versions of amended / revised version of documents made or created should be included in 6.1 above. This applies to both paper and electronic drafts.

6.3 Back-ups:

Records classified as important and/or sensitive by the Chairman and Managing Director / Whole Time Director and CFO, if are in physical formats should be scanned and stored in separate folder file. They alongwith other such electronic records should be subjected to regular back-up by the user or I.T. Department. Backup/Mirror images of the records in I.T. Server should also be ensured, at a separate location(s).

6.4 Retrieval:

Documents must be made accessible to authorised users. Retrieving of documents preserved must be easy and smooth. Creation of appropriate folders and files be ensured. They must be labeled properly to ensure easy and speedy retrieval. Authority to store and retrieve important and sensitive documents be given to atleast two or more senior personnel, who only should have access to drive, folder, files to be stored and it should be password protected.

6.5 Archiving

The documents so preserved in hard papers or in electronic mode, as the case be shall be archived in proper and suitable manner by the administrator, after completion of five years from its creation. Their preservation time limit may be more. These documents, meant for archiving should be kept separately under the control of the administrator, in physical as well as the electronic mode. One or more archival drive, folder, file should be created and maintained with proper authority for access and retrieval.



7. Disposal and Destruction of Records:

Administrator or any employee, duly authorized, in this regard may only destroy or dispose of records in accordance with the normal administrative practice or in accordance to the provisions laid down in statute, whichever is longer.

Confidential records should be destroyed as follows:

7.1 Destruction of paper records

Paper records must be shredded under security. They must never be placed in unsecured bins or rubbish tips.

7.2 Destruction of magnetic media

Records stored on magnetic media such as floppy disks must be destroyed by reformatting at least once. Deleting files from magnetic media is not sufficient to ensure the destruction of the records. Backup copies of the records must also be destroyed.

7.3 Destruction of optical media

Records held on optical media such as rewritable disks must be destroyed by cutting, crushing or other physical means.

