BMD SECURITIES LIMITED

DATA DISPOSAL AND RETENTION POLICY

Policy created by	Designated Officer
Policy reviewed by	Technology Committee
Policy reviewed on	31-12-2024
Policy Approved by	Board of Directors
Policy approved on	28-04-2025

Version – 1.2

Purpose

The purpose of this policy is to detail the procedures for the retention and disposal of information to ensure that we carry this out consistently and that we fully document any actions taken. Unless otherwise specified the retention and disposal policy refers to both hard and soft copy documents. This Policy is also for the purpose of aiding employees in understanding their obligations of retaining electronic documents - including email, text files, digital images, sound and movie files, PDF documents, and all Microsoft Office or other formatted files or paper documents.

Review

This policy defines the Data retention and destruction schedule for paper and electronic records. The Data Retention Schedule is approved as the initial maintenance, retention and disposal schedule for the physical (paper) and electronic records. The Technology committee of Company is responsible for the administration of this policy and the implementation of processes and procedures. In continuation with SEBI guidelines, the Designated Officer is also authorized to; make modifications to the Record Retention Schedule as needed to ensure that it is in compliance with SEBI regulations; ensure the appropriate categorization of documents and records on behalf of the company annually review the policy; and monitor compliance with this policy. Review is the examination of closed records to determine whether they should be destroyed, retained for a further period or transferred to an archive for permanent preservation.

How long we should keep our paper records -

- ✓ Records should be kept for as long as they are needed to meet the operational needs of the Authority, together with legal and regulatory requirements. We have assessed our records to:
  - Determine their value as a source of information about the Authority, its operations, relationships and environment
  - Assess their importance as evidence of business activities and decisions
  - Establish whether there are any legal or regulatory retention requirements
- ✓ Where records are likely to have a historical value, or are worthy of permanent preservation, we will transfer them to the National Archives after 25years.

Responsibilities of Employees –

All employees are responsible for:

- ✓ checking that any information that they provide in regard to their employment is accurate and up to date.
- ✓ informing the regulatory authority of any changes to information, which they have provided i.e. changes of address
- ✓ Checking the information that the Organization will send out from time to time, giving details of information kept and processed about employees.
- ✓ Informing Designated Officer of any errors or changes. The Company cannot be held responsible for any errors unless the employees has informed the management of them.

Disposal schedule

- ✓ A disposal schedule is a key document in the management of records and information.
- ✓ Records on disposal schedules will fall into three main categories:
  - Destroy after an agreed period – where the useful life of a series or collection of records can be easily predetermined (for example, destroy after 3 years; destroy 2 years after the end of the financial year).
  - Automatically select for permanent preservation – where certain groups of records can be readily defined as worthy of permanent preservation and transferred to an archive.
  - Review is the examination of closed records to determine whether they should be destroyed, retained for a further period or transferred to an archive for permanent preservation.
- ✓ Records can be destroyed in the following ways:
  - **Destruction**
    - ❖ Non-sensitive information – can be placed in a normal rubbish bin
    - ❖ Confidential information – cross cut shredded and pulped or burnt
    - ❖ Highly Confidential information – cross cut shredded and pulped or burnt
- ✓ Electronic equipment containing information - destroyed using kill disc and for individual folders, they will be permanently deleted from the system.
- ✓ Destruction of electronic records should render them non-recoverable even using forensic data recovery techniques.
- ✓ **Archival transfer**
  - ❖ This is the physical transfer of physical records to permanent custody at the National Archives Office.

Sharing of information

- ✓ Duplicate records should be destroyed. Where information has been regularly shared between business areas, only the original records should be retained in accordance with the guidelines mentioned above. Care should be taken that seemingly duplicate records have not been annotated.
- ✓ Where we share information with other bodies, we will ensure that they have adequate procedures for records to ensure that the information is managed in accordance with the Authority's policies, relevant legislation and regulatory guidance.
- ✓ Where relevant to do so we will carry out a data privacy impact assessment and update our privacy notices to reflect data sharing.

Data Security

- ✓ All employees are responsible for ensuring that: Any personal data which they hold is kept securely. Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorized third party.

- ✓ Employees should note that unauthorized disclosure and/or failure to adhere to the requirements set out above will usually be a disciplinary matter, and may be considered gross misconduct in some Data cases.
- ✓ Personal information should be; kept in a locked filing cabinet; or in a locked drawer; or if it is computerized, be password protected; or when kept or in transit on portable media the filesthemselves must be password protected.
- ✓ Personal data should never be stored at employees' homes, whether in manual or electronic form, on laptop computers or other personal portable devices or at other remote sites.
- ✓ Ordinarily, personal data should not be processed at employees' homes, whether in manual or electronic form, on laptop computers or other personal portable devices or at other remote sites. In cases where such off-site processing is felt to be necessary or appropriate, the agreement of the relevant Data Controller must be obtained, and all the security guidelines given in this document must still be followed.
- ✓ Data stored on portable electronic devices or removable media is the responsibility of the individual employee who operates the equipment.

An Audit Trail

- ✓ You do not need to document the disposal of records which have been listed on the records retention schedule. Documents disposed out of the schedule either by being disposed of earlier or kept for longer than listed will need to be recorded for audit purposes.
- ✓ This will provide an audit trail for any inspections conducted by the regulatory and will aid in addressing Freedom of Information requests, where we no longer hold the material.

Monitoring

- ✓ Responsibility for monitoring the disposal policy rests with the designated officer. The policy will be reviewed annually or more often as required.

Change in the Policy will be adopted as and when required by the company and is binding on all the Employees/Employees/and Directors of the Company.

BMD Securities Limited

Utpal Mallick
CISO
Dated: - 30-04-2025