



**CENTRAL BANK OF INDIA
PLANNING DEVELOPMENT OPERATIONS
DEPARTMENT
CENTRAL OFFICE
MUMBAI**

**RECORD MAINTENANCE POLICY OF THE BANK
(UPDATED UPTO 31st DEC – 2022)**

INDEX

Sl No	Particulars	Page No	
		From	To
1	Index	1	1
2	Preamble & preview	2	6
3	Policy Statement	7	7
4	Scope	7	8
5	Regulatory Framework	8	8
6	Relationship with other policies	8	8
7	Record classification system & storage	9	11
8	Human Resources Record	12	12
9	Electronic correspondence record	12	12
10	Outsourcing	13	21
11	Disposal of record and Preservation of documents	22	30
12	Access & security	31	31
13	Functional Responsibility at Branches and Administrative Offices	32	35
14	Training	36	36
15	Monitoring & review	36	36
16	Audit & Compliance	37	37
17	Annexure-I Types of record	38	39
18	Annexure-II Duplicate vouchers	40	40
19	Annexure-III File plan	41	42

1.0 PREAMBLE

The Bank is required to manage its record at various levels in a well-structured record keeping system and also have the necessary policy and procedures in place to ensure that the record management practices comply with the requirements of the Acts & statutes.

In terms of the Master Directions of Reserve Bank of India vide RBI/DBR/2015-16/18 Master Direction DBR.AML.BC.No.81/14.01.001/2015-16, updated as on 10th may 2021, stipulates steps to be taken regarding maintenance, preservation and reporting of customer account information, with reference to provisions of PML Act and Rules. Regulated Entities (REs) shall, (a) maintain all necessary records of transactions between the RE and the customer, both domestic and international, for at least five years from the date of transaction; (b) preserve the records pertaining to the identification of the customers and their addresses obtained while opening the account and during the course of business relationship, for at least five years after the business relationship is ended; (c) make available the identification records and transaction data to the competent authorities upon request; (d) V-CIP Records and Data Management-i) The entire data and recordings of V-CIP shall be stored in a system/systems located in India. Res shall ensure that the video recording is stored in a safe and secure manner and bears the date and time stamp that affords easy historical data search. ii) The activity log along the credentials of the official performing the V-CIP shall be preserved.

It further directs banks to introduce a system of maintaining proper record of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005); (d) maintain all necessary information in respect of transactions prescribed under PML Rule 3 so as to permit reconstruction of individual transaction, including the following: (i) the nature of the transactions; (ii) the amount of the transaction and the currency in which it was denominated; (iii) the date on which the transaction was conducted; and (iv) the parties to the transaction. (e) evolve a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities; (f) maintain records of the identity and address of their customer, and records in respect of transactions referred to in Rule 3 in hard or soft format.

Further in terms of Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005), which stipulates Maintenance of records of transactions (nature and value) as

Every reporting entity shall maintain the record of all transactions including, the record of

- (A) All cash transactions of the value of more than rupees ten lakhs or its equivalent in foreign currency;
- (B) All series of cash transactions integrally connected to each other which have been Individually valued below rupees ten lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds an amount of ten lakh rupees or its equivalent in foreign currency;
- (C) All transactions involving receipts by non-profit organisations of value more than rupees ten lakh or its equivalent in foreign currency;
- (D) All cash transactions where forged or counterfeit currency notes or bank notes have been

RECORD MAINTENANCE POLICY OF THE BANK (UPDATED UPTO DEC-2022)

used as genuine or where any forgery of a valuable security or a document has taken place facilitating the transactions;

(E) All suspicious transactions whether or not made in cash and by way of-

- (i) deposits and credits, withdrawals into or from any accounts in whatsoever name they are referred to in any currency maintained by way of:
 - (a) cheques including third party cheques, pay orders, demand drafts, cashiers cheques or any other instrument of payment of money including electronic receipts or credits and electronic payments or debits, or
 - (b) travellers cheques, or
- (c) transfer from one account within the same banking company, financial institution and intermediary, as the case may be, including from or to Nostro and Vostro accounts, or any other mode in whatsoever name it is referred to;
- (ii) credits or debits into or from any non-monetary accounts such as d-mat account, security account in any currency maintained by the banking company, financial institution and intermediary, as the case may be;
- (iii) money transfer or remittances in favour of own clients or non-clients from India or abroad and to third party beneficiaries in India or abroad including transactions on its own account in any currency by any of the following:-
 - (a) payment orders, or
 - (b) cashiers cheques, or
 - (c) demand drafts, or
 - (d) telegraphic or wire transfers or electronic remittances or transfers, or
 - (e) internet transfers, or
 - (f) Automated Clearing House remittances, or
 - (g) lock box driven transfers or remittances, or
 - (h) remittances for credit or loading to electronic cards, or
 - (i) any other mode of money transfer by whatsoever name it is called;
- (iv) loans and advances including credit or loan substitutes, investments and contingent liability by way of:
 - (a) subscription to debt instruments such as commercial paper, certificate of deposits, preferential shares, debentures, securitized participation, interbank participation or any other investments in securities or the like in whatever form and name it is referred to, or
 - (b) purchase and negotiation of bills, cheques and other instruments, or
 - (c) foreign exchange contracts, currency, interest rate and commodity and any other derivative instrument in whatsoever name it is called, or
 - (d) letters of credit, standby letters of credit, guarantees, comfort letters, solvency certificates and any other instrument for settlement and/or credit support;
- (v) Collection services in any currency by way of collection of bills, cheques, instruments or any other mode of collection in whatsoever name it is referred to.
- (F) All cross border wire transfers of the value of more than five lakh rupees or its equivalent in foreign currency where either the origin or destination of fund is in India;
- (G) All purchase and sale by any person of immovable property valued at fifty lakh rupees or more that is registered by the reporting entity, as the case may be.

RECORD MAINTENANCE POLICY OF THE BANK (UPDATED UPTO DEC-2022)

Further in terms of **Right to Information Act, 2005** stipulates that The Act does not require the public authorities to retain records for indefinite period. The records need be retained as per the record retention schedule applicable to the concerned public authority.

In view of the volume of record generated, the space constraints especially in metro and urban areas, most of the corporate have preferred outsourcing the record maintenance i.e. storage in physical & electronic form. This policy details identification of records, classifying record based on file-plan, storing, retrieval, responsibility at various levels, outsourcing, training, audit and checks.

Under the Income Tax Act, 1961, assessment can be reopened within certain period, the maximum period being 10 years. Therefore, under the Income Tax Act, Books of accounts should be maintained for at least 10 years from the end of relevant assessment year.

Record is required to be maintained by the Bank at various levels (Branch Office/Regional Office/Zonal Office/Central Office) for various purposes including and not limited to future reference, giving information to customers, submission to **Court/ALC/RLC/CVC** or any other authority or Statute, audit and inspection.

During the course of normal functioning of the banks, a large volume of record is generated & requires to be preserved for many years. These records are vital for transactional and management information. The enactment of the **Information Technology (IT) Act 2000**, RTI Act 2005, Rent Control Act and change in working of banks has made it imperative for the Bank to review the existing system and procedure on the subject and bring about the necessary improvements in storing/archiving and retrieving record. Technology has brought in vast changes in the method of storing/archiving and retrieving and needs to be adopted for creating and maintaining record to meet Bank's intrinsic and statutory requirements.

Information is a resource of equal importance to management as other standard resources like people, money and facilities. The information resources of our Bank must, therefore, be managed as a valuable asset. Appropriate **record management** is a vital aspect of maintaining and enhancing the value of this asset. The Bank considers its **record to be a valuable asset** to:

- a) Enable Bank to find the right information easily, comprehensively & completely;
- b) Enable Bank to perform its functions successfully and efficiently and in an accountable manner;
- c) Support the business, legal and accountability requirements of the Bank;
- d) Ensure the conduct of business in an orderly, efficient and accountable manner;
- e) Ensure adherence to Statutory/regulatory requirements;
- f) Ensure the consistent delivery of services;
- g) Support and document policy formation and administrative decision-making;
- h) Provide continuity in the event of a disaster;
- i) Protect the interests of the bank and the rights of employees, clients and present and future stakeholders;
- j) Support and document the Bank's activities, development and achievements.

Record management through the proper control of the content, storage and volume of record, reduces vulnerability to legal challenge or financial loss and promotes best value in terms of human and space resources through greater co-ordination of information and storage systems.

Accordingly a comprehensive policy on Record Maintenance by Bank has been prepared for the perusal and approval for the Board of Directors of the Bank

1. Preview:

- a. The policy is regarding preservation of Bank's documents/records in line with the applicable law. This policy ensure that the Bank's business is adequately documented and managed in accordance with best practices. This Policy documents that all necessary documents and records of the Bank are adequately protected and preserved as per the statutory requirements and that the records of the Bank which are no longer required or are of no value are disposed off after following due process for discarding the same. This Policy also envisages the purpose of aiding staff of the Bank in understanding their obligations in retaining and preserving the documents and records which are required to be maintained as per the applicable statutory provisions and regulatory requirements.
- b. For the purpose this policy, the **Documents/ Records** herein shall mean all Papers, Files, Vouchers, Registers, Ledgers, Cash Scrolls, Manuals, Agreements, Paid Cheques, Drafts, Orders, Declarations, Forms, Books, Tapes, Floppies, CDs, DVDs, all types Electronic Storage Devices, etc. and the like as required to be maintained by the Bank under any applicable law or regulation for the time being in force or in existence, maintained in physical or electronic form or both and does not include multiple or identical copies.
- c. Further "**Electronic Record(s)**" means the electronic record as defined under section 2 (1) (t) of the **Information Technology Act, 2000** and Electronic Form/s means any contemporaneous electronic devices such as Computer, Laptop, Desktop, Compact Disc, space on electronic cloud or any other form of electronic storage and retrieval device, considered feasible, whether the same is in possession or control of the Bank or otherwise the Bank has control over the access to it.
- d. Since Bank is also listed in the Stock Exchanges, Listing Regulations herein shall mean Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015 ('Listing Regulations').
- e. It the responsibility of all the employees in the permanent rolls of the Bank either in the Bank and/or on deputation are responsible for taking into account the potential impacts on preservation of the documents in their area of work / assignments and their decision to retain/preserve or destroy documents pertaining to their area.

1.1 Document Management:

Record is either in original or copies of correspondence and business forms, or electronic data such as computer tapes and discs. Record includes account opening forms & supporting documents, vouchers, registers, ledgers, statements, correspondence, agreements, invoices, licenses, certificates, photographs, films and other kinds of documents. Record is

RECORD MAINTENANCE POLICY OF THE BANK (UPDATED UPTO DEC-2022)

information of the bank created and maintained in the course of business. Record can be in any media including paper, electronic storage device. Work-related record, including e-mail, that employee produces at home and on personal home computers/laptops is also the property of the bank, **hence such official mails/ data created/ generated is required to be transferred on to the Bank's system, which shall be treated under the definition of Record.** Record is unique as it is evidence specific to a transaction, customer, correspondence, property, security, etc.

1.2 Record Management:

Record management encompasses the methods, processes, procedures & practices relating to and the associated reporting on the creation , cataloguing, sorting, storing, distributing, duplicating, converting, safekeeping, tracking, linking and destruction of record.

1.3 Information Creation:

Record is created through internal employees' activities and from external transactions and correspondence.

1.4 Distribution and Use:

Information is shared between employees and used for decision; evidence and other business purposes. Media vaulting is still used to protect electronic assets. The Bank may utilize Imaging to create retrieval record of enterprise documents, paper record kept under open shelf filing etc. Imaging, storing of data which is preserved in electronic form, files, vouchers, etc. can be preserved at locations of third parties to lower the operating costs with adequate security.

1.5 Storage and Maintenance:

Information that has lived through its immediate use continues to have high reference potential. The Bank may elect to use Offsite record Storage for such record in combination with a Scan on Demand or faxing Service to facilitate retrieval. The record may also be maintained Offsite using Open Shelf Filing.

1.6 Retention and Disposition:

Information and record need to be retained/preserved due to statutory requirements, for legal or audit protection or due to standard industry practice. Offsite Record Storage could be used to store old record at lower cost maintaining security and tracking system to facilitate retrieval. Tape, CD or DVD libraries may also be stored in Media Vaults. The information / record shall be destroyed as permitted in the policy.

1.7 Archival Preservation:

The preservation of some record/information requiring permanent retention can be on digital mode or scanning for long term preservation or maintenance of original paper record in an Environmentally Controlled Vault or Climate Controlled Record Center.

2. POLICY STATEMENT

2.1 All record created and received by the Bank shall be managed in accordance with best practices of Corporate Governance.

2.2 The following broad principles shall apply to the record keeping and record management practices of the Bank:-

- The Bank shall follow sound procedures for the creation, maintenance, retention and disposal of all record, including electronic record;
- The record management procedures of the Bank shall comply with legal requirements, including those for the provision of evidence;
- The Bank shall follow sound procedures for the security, privacy, confidentiality & integrity of its record;
- Electronic record in the Bank shall be managed as enumerated by RBI & IBA;
- The Bank shall have performance measures for all record management functions and shall review compliance with these measures.

3. SCOPE

3.1 This Policy impacts upon Bank's work practices for all those who

- Create record including electronic record;
- Have access to record;
- Have any other responsibility(s) as regards storage and maintenance;
- Have management responsibility(s) for the staff engaged in any of these activities; or manage, or have design input into information technology infrastructure;
- Are rendering services outsourced by the Bank.

3.2 The Policy, therefore applies to all staff members of our Bank and covers all record regardless of format, medium or age.

This policy document deals with record maintenance in four sections as under:

- a) Record keeping – Type of record
- b) Record Retention – Period/Duration
- c) Record Media – Physical / scanned & securely coded
- d) Record Retrieval – Physical / scanned / procedure

Requirements set out in this Policy or other instructions which may be issued from time to time in relation to record maintenance shall be in addition to and not in derogation of such requirements which are required to be complied with by banks as per law in force. The Branch/Regional/Zonal/Central Office management shall be responsible to ensure compliance of all statutory provisions as stipulated in various Acts and Rules.

Apart from the legal requirements to be met under various statutes, The Bank while storing electronic data shall take into account the policy guidelines issued by the Reserve Bank of India, to the extent relevant, on (i) guidelines on risk and control in computer and telecommunication system; (ii) guidelines on Internet banking; (iii) guidelines on

RECORD MAINTENANCE POLICY OF THE BANK (UPDATED UPTO DEC-2022)

Information System Audit Policy for Banking and Financial Sector; (iv) Check-list on Information System Audit; (v) IT Security Policy.

- 3.3 The scope for preservation of records has been expanded to include Credit Guarantee Scheme of Credit Guarantee Fund Trust for Micro and Small Enterprises (CGTMSE), Deposit Insurance and Credit Guarantee Corporation (DICGC), Export Credit Guarantee Corporation of India Limited (ECGC) or any such scheme in future as well.

4. REGULATORY FRAMEWORK

- 4.1 By managing its paper based record effectively and efficiently, the Bank shall strive to give effect to the accountability, transparency and service delivery values contained in the legal framework established by:

- Indian Evidence Act, 1872
- Bankers Book Evidence Act, 1891
- Reserve Bank of India Act, 1934
- Banking Regulations Act, 1949
- Companies Act, 2013
- Income Tax Act, 1961
- Banking Companies Act (Period of Preservation of Record) Rules, 1985
- Information Technology Act, 2000
- Prevention of Money laundering Act, 2002
- Prevention of Money Laundering (Maintenance of Records) Rules, 2005
- Right to Information Act, 2005
- SEBI Act

5. RELATIONSHIP WITH OTHER POLICIES

- 5.1 Electronic Record Maintenance Policy, E-mail Policy, Document Imaging Policy, and Web Content Management Policy shall be the complimenting policies to cover the unique nature of the broad spectrum of record generated by the Bank and the same after preparation by Department of Information Technology and approval thereof from the Board of Directors shall be a part of this Policy.

- 5.2 Other policies related closely to the Record Maintenance Policy are:
- Information Security Policy (managed by the Chief Information Security Officer)
 - Internet Usage Policy (managed by the DIT); and
 - Policy on Access to Information (managed by the DGM-OPR at Central Office and all designated Executives at Zonal level).

6. RECORD CLASSIFICATION SYSTEM AND STORAGE

- 6.1 File plan drawn so that there is systematic storage & retrieval of data. The file plan shall be used for the classification of paper based and electronic (including e-mail) record.
- 6.2 Specific procedures for the allocation of file subjects and reference numbers to electronic record and procedures manual shall be designed and published on the Intranet for immediate reference of all concerned. Likewise, specific guidance regarding the classification of e-mail shall be contained in the E-mail Management Policy.
- 6.3 Each staff member shall allocate file reference numbers to the record according to the approved subjects of the file plan. However, in respect of the record for which no subject exists in the file plan, the record manager shall be contacted for additions to the file plan. Under no circumstances new subjects shall be added to this file plan without the approval of the record manager.
- 6.4 Paper-based correspondence files shall be kept in the custody of Daftary.
- 6.5 All offices shall have Record Room/fire proof store-well for safe keeping record.
- 6.6 All paper-based correspondence and record that are not HR related shall be housed in the record room.
- 6.7 All the record shall be under the management of the record manager with the mandate to ensure proper maintenance.
- 6.8 The Record Room is a secured storage area and only Record Room staff shall be permitted in the record storage area.
- 6.9 Staff members who need access to files in the Record Room shall place a request for the files.
- 6.10 The Record Room shall be locked when not in operation.
- 6.11 **Paper based**
 - The Bank shall have record room for paper-based record, at each office, under the control of the record manager with mandate to ensure proper maintenance.
 - The record relating to the correspondence shall be in the custody of the officials that use them on daily basis.
 - For all-important record viz. ownership of properties, share certificates, record of similar nature, etc. which is required to be kept perpetually, shall be kept at Central Office Record Room at Central Office level.
 - Where storage places are not available or are not economically viable, the record keeping may be outsourced as per the designated Central Office outsourced vendor
 - For Fire Safety, all Record Rooms shall be provided with fire-fighting equipment. All large godowns / warehouses shall be provided with **fire alarm system** with auto-dialer. If Record Rooms are not manned 24X7, provision of Automatic modular extinguishers shall be considered.
 - All precautions should be taken to preserve the records, invariably implying that necessary infrastructure also need to be preserved.
 - For safety of record there shall be proper **access control**.
 - Grill gate, grills on windows, shutter at the main entrance, exhausts and ventilators shall be installed.

RECORD MAINTENANCE POLICY OF THE BANK (UPDATED UPTO DEC-2022)

- Regular **pest/rodent control** shall be provided.
- Proper insurance shall be taken of the infrastructure.
- **Cleanliness**, including dusting of boxes etc. on day to day basis may be done in the Record Room godown. There should be proper disposal of waste papers. As provided in law, 'No smoking' boards may be displayed and smoking shall be strictly prohibited. For large godowns, there shall be a night watchman/security guard.

6.12 Micrographic/scanning of record:

Record may be micro-filmed, based upon the requirements, and shall be under the control of the Record Manager with mandate to ensure proper maintenance.

6.13 Most of the record is to be held either in paper form or as electronic data. The record beyond the period of preservation period detailed in Bankers Book of Evidence Act, may be held in digital form or by way of document scanning/micro filming with specific permission of respective Departmental Head, Zonal/Regional Manager (as per authority delegated specifically).

6.14 Where the underlying paper documents are subsequently destroyed and the converted format becomes the prime record, a certificate of authenticity shall be produced at the time of conversion and shall be signed by the official responsible for overseeing the conversion process.

6.15 **Audio-Visual (AV) record:** based on the requirements, AV record shall be stored and shall be under the control of the record manager who is mandated to ensure proper maintenance.

6.16 Electronic System other than the correspondence.

6.16.1 Our Bank has a number of electronic record in operation which is not part of the correspondence.

6.16.2 The IT manager shall be responsible for the day-to-day maintenance of electronic record.

6.16.3 The record maintained in the electronic form shall be under the control of the record manager of the IT Department who is mandated to ensure proper maintenance.

6.16.4 Detailed guidance regarding the management of electronic record shall be incorporated in the Electronic Record Maintenance Policy.

6.17 Legal admissibility and evidential weight: The record of the Bank shall at all times contain reliable evidence of business operations. The following shall apply:

(1) Paper-based record

- No record shall be removed from paper-based files without the explicit permission of the record manager.
- Record that was placed on files shall not be altered in any way.
- No alterations of any kind shall be made to record other than correspondence files without the explicit permission of the record manager.
- In case of evidence of tampering with record, the staff member involved shall be subject to disciplinary action.

(2) Electronic record

- The Bank shall use system which ensures that its electronic record is authentic; not altered or tampered with; auditable; and produced in system which utilizes security measures to ensure integrity. The Electronic Record Maintenance Policy shall contain specific information regarding the metadata and audit trail information that should be captured to ensure that record is authentic.

(3) Off shore record

- The regulatory authority of the offshore location does not have access to the data relating to Indian operations of the Bank simply on the ground that the processing is being undertaken there (not applicable if off-shore processing is done in India)
- RBI Inspectors (and external auditors) will be permitted to visit and carry out examinations at the offshore location.
- Where the offshore service provider is a regulated entity, the relevant offshore regulator will not obstruct the arrangement nor object to RBI inspection visits.
- If data processing at the offshore location is outsourced to a service provider which is not a regulated entity, the controllers, directors and managers of the service provider are fit and proper people to be providing such services to Bank.
- The availability of record to management and the RBI will withstand the liquidation of either the offshore custodian or the Bank.
- With the increasing and extensive use of computers and other electronic gadgets in the banks most of the above record maintained by them will be available both on the paper based and electronic media. All the staff members should, however, note carefully that the statutory provisions regarding record maintenance as per various acts are applicable evenly for the paper based record as well as for the electronic media record. It is, therefore, imperative on the staff members particularly Supervisory staff, to properly understand the provisions under this guideline paper and act scrupulously in the matter of record maintenance.

7.0 HUMAN RESOURCES RECORD

- 7.1 All Human Resources related record shall be housed separately.
- 7.2 The general HR subject files as well as HR case files shall be under the management of the record manager with mandate to ensure proper maintenance.
- 7.3 Bank shall maintain a set of paper-based files for each employee. These files shall be confidential in nature and shall be housed in a secure storage area in the HR Record Room.
- 7.4 The office files shall be managed as part of the List of Series of Separate Case Files that shall be maintained and managed by the record manager.
- 7.5 The files exist only in paper based format and the physical tracking of the case files shall be managed with the file tracking system in the Integrated Document and Record Management System.

8.0 Maintenance of Electronic Documents/ Correspondence Records :

Maintenance of Electronic Documents/ Correspondence Records shall be stored in an electronic repository maintained by the IT Section.

- 8.1 Access to storage areas where electronic record is stored shall be limited to the Information Technology staff having specific duties regarding the maintenance of the hardware, software and media.
- 8.2 The record manager shall maintain a schedule of all record other than the correspondence system. The schedule shall contain a description of each set of record other than the correspondence system and indicate the storage location and retention period of the record regardless of format. The schedule shall be made available on the Intranet.
- 8.3 Should record be created / received that is not listed in the schedule, the record manager shall be contacted to add the record to the schedule.
- 8.4 **i. KYC documents used for account opening: PAN & OVD documents like Aadhaar, Driving License , Voter ID, Passport, Job card issued by NAREGA & NPR scanned & uploaded at branch level should be maintained electronically.**
- ii. OMs, other documents of all the departments on-boarded to DMS platforms to be maintained electronically.**
- iii. Documents of all departments processed under Archival Solution module of DMS should be maintained electronically.**

9. OUTSOURCING

9.1 In case banks record is warehoused in a facility managed by an outsourced agency, the bank has to ensure that all requirements as regards safety, security and availability are met fully. Facility should be subject to security under IS Audit and also should be available for RBI inspection.

9.2 Evaluating the capability of the Service Provider.

9.2.1 In considering or renewing an outsourcing arrangement, appropriate due diligence should be performed to assess the capability of the service provider to comply with obligations in the outsourcing agreement. Due diligence should take into consideration qualitative and quantitative, financial, operational and reputation factors. Banks should consider whether the service providers' system is compatible with their own and also whether their standards of performance including in the area of customer service are acceptable to it. Where possible, the bank should obtain independent reviews and market feedback on the service provider to supplement its own findings.

9.2.2 Due diligence should involve an evaluation of all available information about the service provider, including but not limited to:-

- Past experience and competence to implement and support the proposed activity over the contracted period;
- Financial soundness and ability to service commitments even under adverse conditions;
- Business reputation and culture, compliance, complaints and outstanding or potential litigation;
- Security and Internal control, audit coverage, reporting and monitoring environment, Business continuity management.
- External factors like political, economic, social and legal environment of the jurisdiction in which the service provider operates and other events that may impact service performance.
- Ensuring due diligence by service provider of its employees.

9.3 Roles and Responsibilities - Service Provider

9.3.1 Collection

The Service Provider will visit different branches/offices of the bank for collection of non-current record/documents in physical form i.e. files, bound vouchers bundles, registers, ledgers etc. for storage at Record Storage Centre (RSC) in a time bound programme which will be decided mutually. The requirement includes the packing of boxes and indexing of contents and all other works or process necessary in this

RECORD MAINTENANCE POLICY OF THE BANK (UPDATED UPTO DEC-2022)

connection. The Service Provider shall carryout collection on specific authority or instructions of the Bank (BM/Dept Head or his authorized representative) in writing/mail from Office ID. The list of inventory will be treated as a Branch document and shall be kept in safe custody, preferably in a fire proof safe.

9.3.2 Cataloguing

The Service Provider will arrange and catalogue the bank's records and prepare inventory using bar code technology. Bar codes are to be securely fixed on each carton and its each and every content (files, bound voucher bundles, registers, etc) to prevent any loss during storage or removal/retrieval. Acknowledgments of the records giving the number of cartons / container with description and number of files/registers/bound vouchers bundles, etc. in each box / container are to be given to the concerned branch/office at the time of pickup. Thereafter the Service Provider shall give the soft copy and hard copy of list of inventory. Bar coding should be tamper/water proof.

9.3.3 Transport

The Service Provider will arrange lifting of non-current records, as provided by the bank, from the bank's premises by their own transport facility for storage at RSC. The Service Provider must comply with the local traffic, health, safety and other legislative requirements during transport.

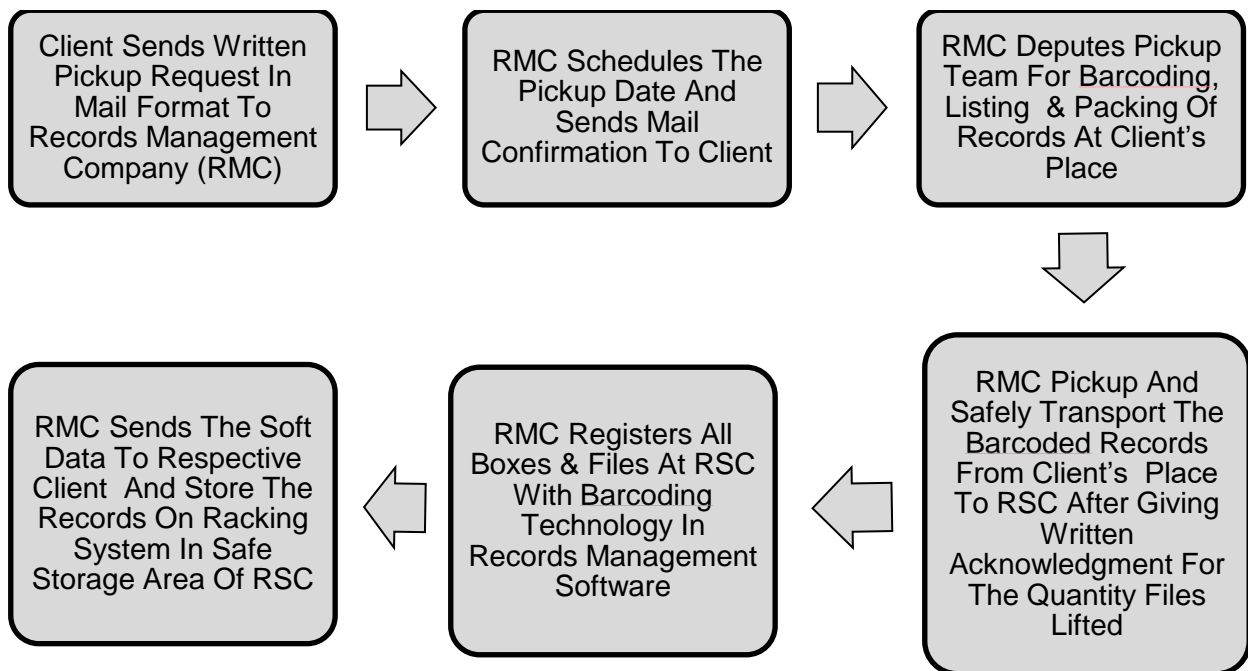
9.3.4 Storage

The Service Provider will provide RSC satisfying the following minimum requirements on shared basis for the Bank.

- The building/structures for storage facility should be a permanent construction preferably on a three feet plinth with RCC/Strong and Corrosion Resistant modern metal roofing, specially designed to protect Bank's records from fire, theft, dust and having proper drainage provision.
- No leakage from water pipes sprinklers, mechanical installations, roots, drains, or any other source of water ingress.
- Storage facilities must be locked and guarded 24 X 7. No unauthorized personnel can be allowed access to the bank's records at any time. Access be controlled by card based/bio metrics electronic access control system and a record kept on register of personnel and material entering and leaving the secured area.
- **Preservation of CCTV recording to be modified as per latest RBI Guidelines as well as Security Policy of the Bank. (90 days for normal Branches and not less than 180 days in case of branches with lockers.**
- Fire protection system to include Fire alarm system, Fire Extinguishers, including modular extinguishers, in accordance with relevant local standards should exist. The Service Provider's staff should be adequately trained in handling fire equipment.
- Service Provider must confirm that Pest and Rodent Control and Termite treatments are carried out regularly in the storage space for a Pest Free environment.
- The Building for storage must be constructed in accordance with local relevant legislations. Service Providers are required to demonstrate/provide evidence of legal ownership or lease of the storage facility with approved site/building plan
- Service Providers are required to use any racking system of reputed company.
- The Service Provider should have E.S.I.C., P.F. registration and hold Labor License. Photocopies of valid registrations and license should be furnished with the Tender.

RECORD MAINTENANCE POLICY OF THE BANK (UPDATED UPTO DEC-2022)

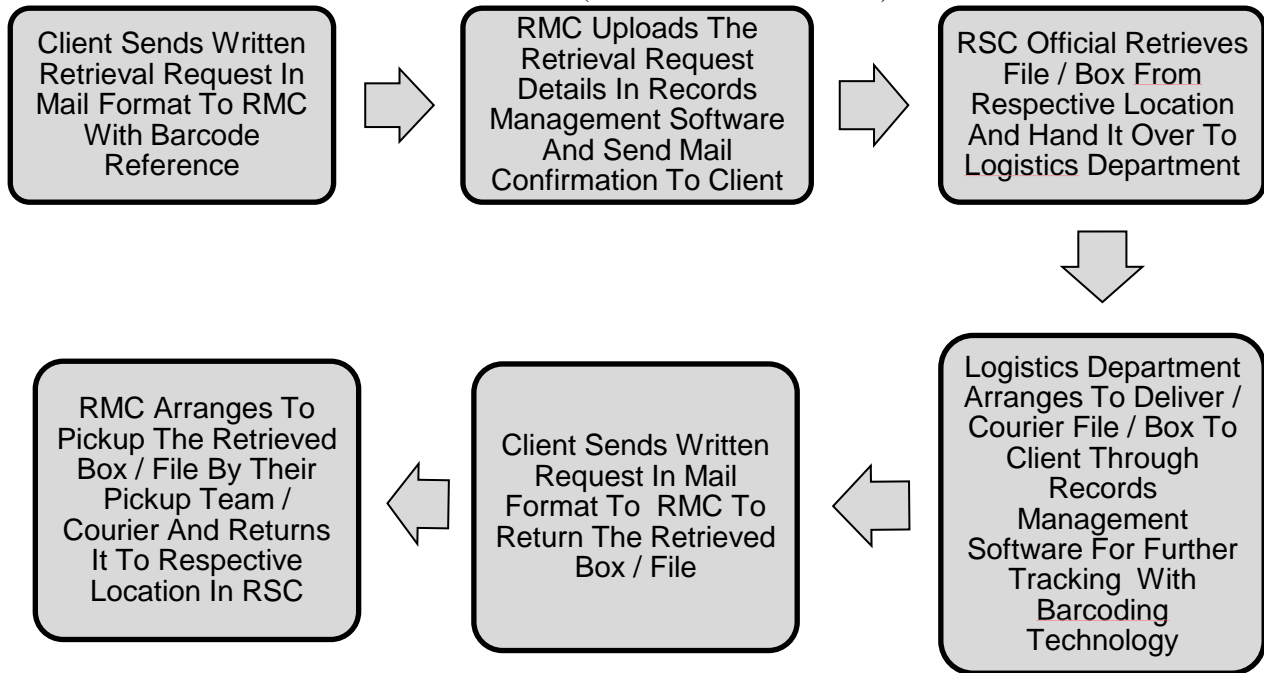
- The storage cartons must be dust resistant with flaps or a lid forming a seal against airborne particles as per following specifications.
- Carton design: 5 ply die-cut bottom minimum Size: 42 cms x 32.5 cms x 26 cms with corresponding 3 ply die-cut top lid with tuck-in on the top on the width sides.
- The bar coding, indexing, packing etc of the records should be done in Bank’s location under supervision of a Bank staff. All cartons should be filled to the top level. The annual check of the documents in custody of the Service Provider will also be ensured to ensure correct quality and quantity of documents. Audits through the ZAO, CA and Third party (when desired) will also help in ascertaining the adequacy of storage. The record of documents help with the Service Provider will be maintained in hard and soft form and a copy of each will also be provided to the Branch/Dept concerned. Storage area should be insured against fire, flood, cyclone and other natural calamity besides theft, burglary etc. and the Service Provider will bear the cost of such insurance. Photocopies of valid insurance policy should be furnished at the time of checking as per policy. The aspects of safety of records through rugged and appropriate construction and the functional responsibilities have been covered at the paragraph on “Storage” above.
- Board properties: Top minimum 180 GSM 24 BF paper and rest 140 GSM 20 BF.
- The Service Provider is required to operate the facility of storage of non-current records of banks in accordance with local legislative requirement in respect of health and safety legislation, employment law, fire safety law, relevant building codes.
- The bank’s representative / security official/RBI representative reserves the right to inspect the RSC to confirm compliance at any time.



9.3.5 **Retrieval of Records**

The Service Provider undertakes to retrieve and deliver the requested cartons, files, vouchers, ledgers, registers and any other documents within below specified TAT upon receipt of a written request in the form of faxes, e-mails or letters from the authorized officials of the bank. Retrieval shall mean delivery to the bank’s premises at different locations.

RECORD MAINTENANCE POLICY OF THE BANK (UPDATED UPTO DEC-2022)



9.3.6 The Service Provider should have implemented a Comprehensive Records Management Software. The Service Provider should have the ability to provide the reports as mentioned at para above. The Service provider will provide Annual Reports to the Branch/Dept in addition to impromptu reports made available during checks by Audit Team or the team from Branches and depts.

9.3.7 **Turn-Around-Time (TAT)**

Nature of Retrievals	Turn-Around-Time (TAT)
Ordinary Retrievals	All requests by fax/ e-mail received by 5 P.M. will be delivered by the next working day to local branches/courier. (24 working hrs TAT)
Urgent Retrievals	All requests by fax/ e-mail received by 12.00 noon will be delivered on the same day to local branches/courier. (A maximum request of 25 files will be entertained at one time. For request over & above this, the delivery will be on best effort basis)
Bulk / Project Retrievals	As communicated by the bank at the time of assigning the task (with mutual consent)

9.3.8 **Retention of Records**

The Service Provider will retain and maintain the records as per Record Maintenance Policy of the bank which shall be provided by the bank.

9.3.9 **Destruction/Permanent Retrieval of Non-Current Records**

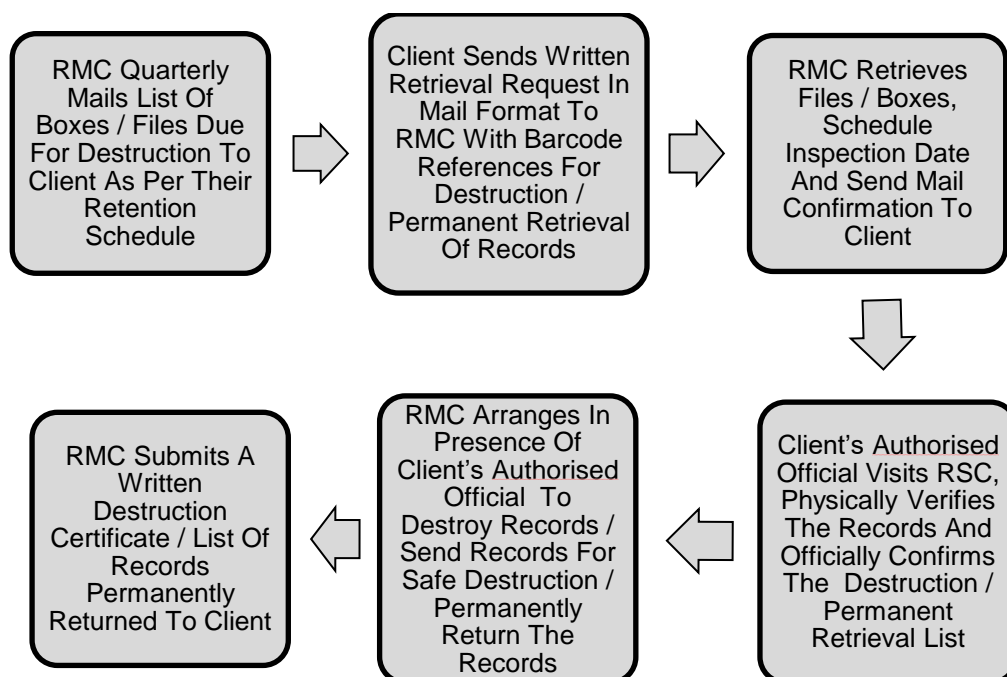
The Service Provider through the Record Management Software will be able to generate a list of documents that are due for destruction based upon the Retention Policy. Thereafter the following procedure will be followed:-

- In the beginning of each quarter (January, April, July, October), the Service Provider will prepare the List of records, which have outlived their retention period in terms of

RECORD MAINTENANCE POLICY OF THE BANK (UPDATED UPTO DEC-2022)

Records Maintenance Policy and inform the concerned branch/office and seek their written consent for destruction.

- Unless there are instructions to the contrary, non-current records meant for destruction will be shredded / burnt in the presence of authorized bank's officials. Records, which are not of confidential nature, may be sold after shredding to a chemical furnace or paper mill for burning or converting into pulp.
- Mode, date of destruction and details of Bank's authority will be recorded in the system, against each relevant item.
- Amount earned at RSC on account of selling record to the paper mill / scrap dealer for converting into pulp will be credited to Bank's Account in the head of "Miscellaneous Income".
- The Service Provider will arrange for transport, labor and other necessary support to send the non-current records to chemical furnace or paper mill, for burning or converting into pulp.



9.3.10 **Migration of Bank's Record Management Data**

Bank plans to use the RMS system available with the Service Provider. However, in case bank intends to use its own Record Management System (RMS) in future, the Service Provider should provide necessary data to the Bank to facilitate such migration.

9.4 **The Outsourcing Agreement**

The terms and conditions governing the contract between the Bank and the service provider should be carefully defined in written agreements and vetted by a competent authority on their legal effect and enforceability. Every such agreement should address the risks and risk mitigation strategies identified at the risk evaluation and due diligence stages. The agreement should be sufficiently flexible to allow the Bank to retain an appropriate level of control over the outsourcing and the right to intervene with appropriate measures to meet legal and regulatory obligations. The agreement should

RECORD MAINTENANCE POLICY OF THE BANK (UPDATED UPTO DEC-2022)

also bring out the nature of legal relationship between the parties i.e. whether agent principal or otherwise . Some of the key provisions of the contract would be:-

- The contract should clearly define what activities are going to be outsourced including appropriate service and performance standards.
- It must ensure that the Bank has the accessibility to all books, record and information relevant to the outsourced activity to the service provider.
- The contract should provide for continuous monitoring and assessment of the service provider by the Bank so that any necessary corrective measure can be taken immediately.
- A termination clause and minimum periods to execute a termination provision, if deemed necessary, should be included.
- Controls to ensure customer data confidentiality and service providers' liability in case of breach of security and leakage of confidential customer related information.
- Contingency plans to ensure business continuity.
- The contract should provide for the approval by the Bank of the use of subcontractors by the service provider for all or part of an outsourced activity.
- It should provide the Bank with the right to conduct audits, on the service provider whether by its internal or external auditors, or by agents appointed to act on its behalf and to obtain copies of any audit or review reports and findings made on the service provider in conjunction with the services performed for the Bank.

9.5. Confidentiality and Security

9.5.1 Public confidence and customer trust in the bank is prerequisite for the stability and reputation of the Bank. Hence the outsourcing authority of the Bank should ensure the preservation and protection of the security and confidentiality of customer information in the custody or possession of the service provider.

9.5.2 Access to customer information by staff of the service provider should be limited to those areas where the information is required in order to perform the outsourced function.

9.5.3 It should be ensured that the service provider is able to isolate and clearly identify the Bank's customer information, documents, record and assets to protect the confidentiality of the information.

9.5.4 Review and monitor the security practices and control processes of the service provider on a regular basis and require the service provider to disclose to the branches.

9. 6 Monitoring and Control of Outsourced Activities.

RECORD MAINTENANCE POLICY OF THE BANK (UPDATED UPTO DEC-2022)

9. 6. 1 The bank should have in place a management structure to monitor and control its outsourcing activities. It should ensure that outsourcing agreements with the service provider contain provisions to address their monitoring and control of outsourced activities.
9. 6. 2 A central record of all material outsourcing that is readily accessible for review by the Board and senior management of the bank should be maintained. The record should be updated promptly and form part of the corporate governance reviews undertaken by the board and senior management of the Bank.
9. 6. 3 Regular audits by either the internal auditors or external auditors of the bank should assess the adequacy of the risk management practices adopted in overseeing the managing the outsourcing arrangement, the Bank's compliance with its risk management framework and the requirements of these guidelines.
9. 6. 4 Banks should at least on an annual basis, review the financial and operational condition of the service provider to assess its ability to continue to meet its outsourcing obligations. Such due diligence reviews, which can be based on all available information about the service provider should highlight any deterioration or breach in performance standards confidentiality and security, and in business continuity preparedness.
- 9.6. 5 The Service Providers facilities will be visited by a team of officers from the ZO/RO prior to utilizing their services to ascertain suitability for storage. The Audit Team will carry out the audit of the Service Provider once in a year and the CA representative once in 6 months. Apart from the above, the Branch/Department of RO/ZO/CO utilizing the services of the Service Provider will also detail a representative to verify and tally the quality and quantity of records held with the Service Provider at least once a year. A record of the same will be maintained and will be checked during the audit of the Branch/Department.
- 9.6. 6 The vendor certifies compliance to the terms of the RFP and also enters into an agreement with our Bank as a token of acceptance of the terms mentioned therein. The fitness of quality and quantity of records is ascertained through the audit checks and the checks by the Branch/Dept. The records to this effect are preserved and maintained for production when desired by the checking authority. The reports provided by the vendor are as under:-

9. 7. **Reports**

9. 7. 1 The Service Provider is required to provide the centre wise/ branch wise reports to the Branch/Dept as per Bank's requirement and periodicity to the designated offices which will be minimum once a year.

9. 7. 2 Total number and details of the cartons with size containing records of the bank being stored at RSC.

RECORD MAINTENANCE POLICY OF THE BANK (UPDATED UPTO DEC-2022)

- 9.7.3 Total number and details of the bank's cartons/records retrieved (delivered) during a period.
- 9.7.4 Total number and details of the bank's cartons/records returned by the Bank.
- 9.7.5 Total number and details of the bank's cartons/records destroyed.

9.8 Insurance

Stored Material is not insured by Company as ownership of the Records lies with the Customer. The insurance of the records stored has to be entered into by Regional office concerned. The Regional office has to ensure insurance of the premises where records are stored against fire, flood, earthquake, explosion, act of God, act of terrorism, war, rebellion, riots, sabotage or strike and lock out. Transit insurance for the documents in transit is a must.

9.9 Penalties

Turn-Around-Time (TAT) to be maintained at all the time else will attract a penalty as mentioned below:

Ordinary Retrievals

<u>Applicable Condition</u>	<u>Applicable Penalty</u>
95% of the total Retrievals in a month as per TAT	NIL
Less than 95% of the total Retrievals in a month as per TAT	10% of the retrievals billing of the month

Urgent Retrievals

<u>Applicable Condition</u>	<u>Applicable Penalty</u>
Retrievals which are not adhered to in 1 day TAT-will be considered as Ordinary Retrieval	As above.

9.10 Liquidated Damages and Force Majeure

In case the Service Provider fails to provide services as per requirement of the bank, they will forfeit the Initial Security Deposit either in part or full. The Bank will be the final authority to ascertain the veracity of any reason provided by the Service Provider. Notwithstanding the provisions of contract, the Service Provider shall not be liable for forfeiture of its Initial Security Deposit or termination for default, if and to the extent that, it's delay in performance or other failure to perform its obligations under the contract is the result of an event of Force Majeure.

9.11 **Confidentiality and Security**

- 9.11.1 Public confidence and customer trust in the bank is prerequisite for the stability and reputation of the Bank. Hence the outsourcing authority of the Bank should ensure the preservation and protection of the security and confidentiality of customer information in the custody or possession of the service provider.
- 9.11.2 Access to customer information by staff of the service provider should be limited to those areas where the information is required in order to perform the outsourced function.
- 9.11.3 It should be ensured that the service provider is able to isolate and clearly identify the Bank's customer information, documents, record and assets to protect the confidentiality of the information.
- 9.11.4 Review and monitor the security practices and control processes of the service provider on a regular basis and require the service provider to disclose security to the branches.

10. DISPOSAL OF RECORDS

- 10.1 The public record shall not be destroyed, erased or otherwise disposed of in the ordinary course of business without either maintaining a back-up or prior written authorization from the competent authority.
- 10.2 The record shall have disposal schedule based on its requirement. However, necessary permission shall be required before disposal of record as per the delegated authority.
- 10.3 Retention period indicated on the file plan and schedule shall be determined considering Bank's legal obligation and functional needs.
- 10.4 Disposal shall be normally being executed/ undertaken annually in month of December. However, if the situation so warrants, any disposal of records/documents on any other month than December, need to be authorized by the Competent authority as per delegated powers for authorizing disposal of records/document.
- 10.5 **Delegated Powers for disposal of records at Branches/ offices:**

The Powers to take decisions for disposal of various records as per the Policy, and responsibility to adhere to the Policy guidelines & its implementation is delegated and rests with shall be taken by the below mentioned Competent authorities, prior to their execution, to ensure that important document /record is not destroyed inadvertently.

Sr.No	Branch/ Office	Delegated authority for disposal if Records
01	All Branch offices upto Scale-3 (Small, Medium & Large)	Branch Manager or Branch In-charge of respective Branch office
	VLB/ ELB and Specialised Branches (CFB, MCB, SAM, ARB and CCPBs)	Manager (Operations, Credit & Recovery)
02	Regional offices	Manager (Operations, Credit & Recovery and all Dept.,)
03	Zonal Offices	Manager (Operations, Credit & Recovery& all Dept.,)
04	Central Office	Chief / Senior Manager of the Concerned Verticals/ Departments
05	Zonal Audit Offices	Chief / Senior Manager of CIA office
06	Service Support Branches (SSBs)	In-charge of respective SSB
07	Training Colleges/ ZSTCs	Dy. Principal / Faculty Leader
08	All other Offices/ Credit Processing Centres etc.,	Officer In-charge of concerned office

- 10.6 Branch/RO/ZO/CO department shall prepare a detailed MIS to include but not limited to serial number, file details, documents details (Letter Reference no/ date/ addressed to/ subject/ address of sender) prescribed period (To / From), mode of destruction, approval for destruction, signature and remarks of officer in whose presence the record is destroyed. It is to be noted that any disposal of records /documents will have to be mandatorily in presence of two officers with one officer not below the **rank of Branch Manager / Chief Manager in Branches and Chief Manager of Operations Department in RO/ ZO/ CO.**
- 10.7 Non-archival record that are needed for litigation, Promotion of Access to information requests or Promotion of Administrative Justice actions may not be destroyed until such time such time the litigation is in process. However any such decision in the matter for disposal of record/ document, will rest with the Deputy General Manager (Law), Central Office.
- 10.8 Record shall be shredded / destroyed by fire in the presence of a responsible Officer as authorized above. Such record may also be sold to bonafide paper manufacturers as approved by Central Office after obtaining an undertaking from them to turn the material into pulp at once and not allow any of the record to pass to other hands. In no case, however, should record, copies of correspondence containing important and confidential matters be sold to any one, not even to bonafide paper manufacturers. Old record, in no circumstances, shall be sold to middlemen such as dealers in waste papers, hawkers, etc. While disposing off old record as stated above, an authorized officer from the branch / department shall be present and both shall sign in Record Destroyed Register/MIS.
- 10.9 Specific guidelines regarding the procedure to dispose off electronic record should be in line with the Electronic Record Maintenance Policy of the Bank
- 10.10 **Record to be preserved permanently and under no circumstances to be destroyed unless authorized.**
- 10.10.1 Even though it is provided in the law that a certain book / record is to be preserved for a specified number of years only and even if the specific period is over, it cannot be destroyed unless and until it is ensured that the book / record will not be required for future reference for any purpose, such as Court case, enquiry proceedings, dispute, etc. The following record shall not be destroyed even though their prescribed minimum preservation period may have expired, until the closure of the said matter.
- Record relating to the matter under dispute or where dispute is likely to arise;
 - Record/matter on which an action by the Bank is likely to arise or has been taken, shall be preserved till dispute is disposed off or finally settled;
 - Record relating to claim notices received by the Bank or Garnishee Order served on Bank or claim cases filed in respect of deposits etc. in the name of third party(s) or for balance/securities in the account of or articles in safe keeping held in the name of the

RECORD MAINTENANCE POLICY OF THE BANK (UPDATED UPTO DEC-2022)

deceased person(s) should be preserved till Garnishee Order is vacated or till completion of 3 years after the claims are fully settled;

- Record relating to suit, which has been filed, should be preserved till the decree has been realized in full or if challenged further then till disposal of the case or if not challenged then till one year further from the date of limitation to challenge the order.
- Record required to be produced on witness summons should be preserved till they are required;
- Record of correspondence to which important or legal reference may have to be made or when it is anticipated in view of the information or incident that a dispute is likely to arise at a future date should be preserved till they are required;
- All indemnity bonds obtained from customers for procuring duplicate DDs, Banker's Cheques, deposit receipts, etc. in case original instruments being reported lost;
- Records pertaining to outstanding entries in IBR and Nominal/Suspense Accounts;
- Records relating to Interest Suspense Account/ Un-realized Interest;
- Records related to write off proposal and related papers;
- Records relating to Lease Deeds of rented offices/residential premises, including the original Lease Deeds, Purchase Agreements;
- Memorandum Book maintained for recording Equitable Mortgages of properties of customers and staff, even after handling over the title deeds to the customers/staff;
- Records and registers/Books etc. relating to properties, fixed assets, furniture and fixtures, etc.

10.10.2 Classification of documents

The documents / records are classified as under and to be retained and preserved for future as required under the relevant provisions of applicable Law & Rules:

Category A	The documents of permanent nature shall be maintained and preserved permanently by the Bank subject to the modifications, amendments,
Category B	The documents of the Bank to be maintained and preserved for specified time period after completion of the relevant transactions shall be preserved by the Bank for the term not less than Ten year after completion of the relevant transactions subject to the modifications, amendments, addition, deletion or any changes made therein from time to time. Provided that all such modifications, amendments, addition or deletion in the documents shall also be preserved for a term not less than Ten (10) years. Further the Bank may, if deemed fit and possible from time to time, maintain mentioned documents in electronic form, to the extent possible.

Notwithstanding anything contained in this policy:

- (a) In case of dispute with tax authorities or government authorities, records and documents relating to dispute shall be preserved till the settlement of dispute or ten (10) years whichever is later.
- (b) Records pertaining to transactions listed out in Rule 3 of The Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, the Nature and Value of Transactions, The Procedure and manner of Maintaining and Time for Furnishing Information and Verification and Maintenance of Records of the Identity of the Clients of the Banking Companies, shall be maintained for a period of five (5) years from the date of cessation of the transactions between the client/customer and the
- (c) Branch/RO/ZO/CO department has to mandatorily take permission from Deputy General Manager (Law)/ Asst. General Manager (Law) prior to disposal of any record /document relating to any legal case /judicial case/ etc.,
- (d) **Records not falling in any of the above there categories shall be maintained for a period of ten (10) years from the date of cessation of the transactions with the client/customer.**

10.10.3 Mode of Preservation

The documents may be preserved in Physical Form or Electronic Form.

All policies, documents and other information not related to any particular period/ event shall be on display on the Bank's website till they are replaced by an updated version. Thereafter they will be archived and preserved in a secured server of the Bank.

All events or information which, in the opinion of the Board of Directors of the Bank, is material and has hence been disclosed to the stock exchange(s) in terms of Regulation 30 of the Listing Regulations, shall remain on display on the website of the Bank for a minimum period of 5 years or such other limit or time as may be prescribed by the Listing Regulations from time to time and thereafter shall be archived for retrieval for a period of three years after the same is archived. For ensuring safety of the data hosted on the website of the Bank, a backup of the website shall be taken on regular intervals.

10.10.4 Period of Preservation of Bank's Records & Administration

The Record Retention Schedule for initial maintenance, retention and disposal schedule for physical and electronic records is given in the annexure

A. Register

Record Type	Retention Period	Category
Attendance Register	Permanent	A
Leave Register	Permanent	A
Bank Guarantee Register	Permanent	A
Safe Custody Register	Permanent	A
Power of Attorney Register	Permanent	A
Equitable Mortgage Register	Permanent	A
Dormant Account Registers	10 Years	B

RECORD MAINTENANCE POLICY OF THE BANK (UPDATED UPTO DEC-2022)

DD/MT/Registers	10 Years	B
Remittance Registers	10 Years	B
Bill Registers	10 Years	B
Clearing Registers	10 Years	B
Loan / Liability Register	10 Years	B
DD/MT/ advise /Register	10 Years	B
Drawing Power Register	10 Years	B
Stock and Shares Registers	10 Years	B
Balancing Register	10 Years	B
Cheque Book Register	10 Years	B
Cheque Return Register	10 Years	B
Furniture and Fixture Register	10 Years	B
Vault Register	10 Years	B
Premises and Building Register	10 Years	B
Overdue Deposit Register	10 Years	B
Account Receivable / Payable Register	10 Years	B
Stop Payment Register	10 Years	B
Visit Register	10 Years	B
Letter of Credit Register	10 Years	B
Key Movement Register	10 Years	B
Dispatch Register	10 Years	B

B. Scrolls, Cards, Receipts and Books

Record Type	Retention Period	Category
Gold Card Register	10 Years	B
Stock / Pledge Register	10 Years	B
Trust Receipts	10 Years	B
Cash Book/Master Cash Scroll	10 Years	B
Bank Transfer Scrolls	10 Years	B
Subsidiary Day Books/Head Office memo	10 Years	B

C. Ledgers

Record Type	Retention Period	Category
Deposit Ledgers	10 Years	B
Call/Fixed Dep. Ledger	10 Years	B
Other Deposit Ledgers	10 Years	B
Govt. securities Ledger	10 Years	B
Investment Ledger	10 Years	B
Loan Register	10 Years	B

D. Account opening forms, Customer KYC records, Paid instruments, vouchers and other documents

Record Type	Retention Period	Category
Paid cheques/Drafts/Voucher relating to AWB/Pay orders/Div. Warrant/Refund Orders/All payment instruments	10 Years	B
Other vouchers incl. those relating to DD/TT/MT/ AWB/loans and advances including LC and BG etc	10 Years	B
Postal receipts and acknowledgment Receipt and acknowledgment of Swift etc	10 Years	B
Account Opening forms, nomination forms, Standing Instructions etc. of closed accounts	10 Years	B
Account Opening forms in respect of all types of Deposits, Loans & Advances, Foreign Exchange Transactions & Contracts, Remittances, both Inward and Outward (Inland/ Foreign) etc.,	10 years from the date of cessation of transaction between the customer and Bank	B
KYC Records of the Customers	10 years from the date of cessation of account based relationship with the Bank	B

E. Files (including those in Electronic Media)

Record Type	Retention Period	Category
Closed Loan Accounts-Personal files	10 Years	B
Correspondence with branches	5Years	B
Concurrent Audit Reports where all comments are rectified and no comments relating to disciplinary proceedings pending	5 Years	B
RBI inspection Reports where all comments are rectified and no comments relating to disciplinary proceeding is pending	5 Years	B
Detailed Internal Inspection Report file where all comments are rectified and no comments relating to disciplinary proceedings pending	5 Years	B
Personal files of customers	10 Years	B
Confidential files	10 Years	B
Files relating to claims of deceased customers	10 Years	B
Files relating to break opening of lockers/vaults	10 Years	B
General correspondence	5 Years	B
Stop payment Instruction file	10 Years	B
Loan Document files(other than those returned to borrower)	12 Years	B
DICGE/ECGC claim invoked files	12 Years	B
Balance sheet of Bank/Branch	10 Years	B

RECORD MAINTENANCE POLICY OF THE BANK (UPDATED UPTO DEC-2022)

Long Form Audit Report	10 Years	B
Charge Taking Reports	10 Years	B
Files on Unclaimed Accounts	10 Years	B
Files relating to Income Tax, Tax deducted at source etc.	10 Years	B
Licenses, sanctions from RBI/Government/local bodies and the like for activities which are concluded and which are no more relevant	10 Years	B
Files relating to Fraud, dispute, suit, attachment orders of court etc. after closure of the matter	12 Years	B
Agreements/deeds related to vacated/disposed land and buildings once used by the bank as quarters or business purpose with bills/receipts of outgoings	10 Years	B

F. Statements & Printouts

Record Type	Retention Period	Category
Flash Data Print outs	1 Year	B
Stock Statements of Customers (other than Pledge)	2 Years	B
Bulletins in bound form/unbound form	5 Years	B
Statements, Exception Reports, ATM Printouts	2 Years	B

G. Electronic Records

Record Type	Retention Period	Category
Images of payment instruments (CTS)	10 Years	B
Tele transfer (including electronic fund transfer) confirmations	10 Years	B
Wire transfer messages and confirmation messages	10 Years	B
Confirmations of E-mail, telegram, telephone, fax etc.	10 Years	B
Backups in floppies/CDs/electronic device	10 Years	B
EXE files- files to run the software	10 Years	B
Source codes creating EXEs	10 Years	B
SWIFT Messages – Inward/outward	10 Years	B

H. Electronic Records

Record Type	Retention Period	Category
Certificate of incorporation, Memorandum/Articles of Association and any Licenses and Permissions	Permanent	A
Listing Agreement	Permanent	A
Common Seal, if required by law	Permanent	A
Minutes of the Board Meeting, various Committees Meetings and General Meetings and Scrutinizer's report	Permanent	A
Statutory Forms and disclosures except routine compliances	Permanent	A
Statutory Registers that may be applicable for listed Banking Company	Permanent	A
Policies Formed by the Bank under various laws and regulations	Permanent	A
Court Orders relating to shareholder matters.	Permanent	A
Register of Members along with the Index	Permanent	A
Other records as may be required under any law(s), from time to time.	Permanent	A
Scanned & uploaded KYC records of the customers.	Permanent	A
OMs & other documents on-boarded & Documents processed under Archival Solution module of DMS.	Permanent	A
The scanned & Uploaded vouchers and formats used for non-financial transactions under Voucher Audit System (VAS)	Permanent	A
Annual Returns and copies of all certificates and documents required to be annexed thereto.	8 Years	B
Books of account and	8 Years	B

RECORD MAINTENANCE POLICY OF THE BANK (UPDATED UPTO DEC-2022)

supporting documents, vouchers, records, contracts, deeds, agreements, etc		
Attendance registers	8 Years	B
All notices under Section 184 of the Companies Act, 2013 read with Rule 9 of the Companies (Meetings of Board and its powers) Rules, 2014.	8 Years	B
Agenda papers, Notice of Board Meeting, Committee Meeting, General Meeting and other related papers.	8 Years	B

I. Video- CIP Records and Data Management:

As per RBI Master Directions on KYC vide RBI/DBR/2021-22/35 & Master Direction DOR.AML.REC.No.15/ 14.01.001/2021-22 updated as on 10 May, 2021, the Video –Customer Identification Process (V-CIP) Recording and Data Management stipulated as under.

(i) The entire data and recordings of V-CIP shall be stored in a system/systems located in India. Bank shall ensure that the video recording is stored in a safe and secure manner and bears the date and time stamp that affords easy historical data search. The extant instructions on record management, as stipulated in RBI’s Master Direction shall also be applicable for V-CIP.

(ii) The activity log along the credentials of the official performing the V-CIP shall be preserved.

Record Type	Retention Period	Category
Video- CIP recordings & Digital on-boarding records and KYC Records obtained from the Customers & activity log and credentials of the officials performing the V-CIP/ Digital On-boarding	10 years from the date of cessation of account based relationship with the Bank.	B

11.0 **ACCESS AND SECURITY**

- 11.1 In case of requisitioning any voucher, the whole bunch of vouchers should be delivered containing the relative voucher as it would not be possible to take out that particular voucher as the same are required to be tied up together.
- 11.2 The record of files / vouchers etc. asked for should be duly entered in the “Record Register”. It should be further verified and ensured, from time to time, that all the record has been received back safe and intact.
- 11.3 If any paper or document is taken out from some file, substitution card/ preferably a photocopy of record taken should be kept on record with proper remarks as to where the document has been sent. It should also be entered like other record in the register and its returning should be ensured.
- 11.4 No staff member shall remove record that is not available in the public domain from the premises of the Bank without the explicit permission of the record manager in consultation with the head of the department / office.
- 11.5 No staff member shall provide information and record that is not in the public domain to the public without consulting the Chief Public Information Officer (CPIO).
- 11.6 No staff member shall disclose personal information of any member of staff or client of the Bank to any member of the public without consulting the Chief Public Information Officer.
- 11.7 An audit trail shall be logged of all attempts to alter / edit electronic record and its metadata.
- 11.8 Record storage areas shall be protected, at all times, against unauthorized access. The following shall apply:
- 11.8.1 Access to server rooms and storage areas for electronic record media shall be managed with key card access;
- 11.8.2 Safe keeping: All the Balance Books, Registers, Ledgers, Files, Security items etc. shall be kept duly locked daily at the close of business hours.

11.9 **Business Continuity Plan**

As the ownership of the document continues to rest with the Dept/ Office, a copy of the document must be maintained in digitized form. For this the services of the Service provider may be sought. Regular checks by the Offices, the Audit Dept and various other functionaries will also help in detecting any lapses that might occur and in taking timely corrective measures. The storage, transportation and retrieval processes will be through reliable and reputed agencies, if not done by the Service provider himself, and these will be the responsibility of the Service Provider.

12. **Functional Responsibility at Branches and Administrative Offices**

12.1 **Overall In-Charge**

- 12.1.1 The General Manager (**PDOD**) shall be overall in-charge for the record keeping and record management practices of Bank.
- 12.1.2 The General Manager (**PDOD**) shall be committed to enhance accountability, transparency and improvement of service delivery by ensuring the sound record management practices are implemented and maintained.
- 12.1.3 The DGM/AGM (**OPR**) shall support the implementation of this policy and ensure that each staff member supports the values underlying in this policy
- 12.1.4 The Dy./Asst. General Manager (OPR) shall designate a Chief/Senior Manager to be the record manager of the Bank and shall mandate the Record Manager to perform such duties as are necessary to enhance the record keeping and record management practices of Bank to enable compliance with legislations and regulations.
- 12.1.5 He shall from time to time issue circulars and instructions regarding the record keeping and record management practices of Bank. He shall make training and other interventions as are necessary to ensure that Bank's record keeping and record management practices comply with the record management principles.
- 12.1.6. The delegated authorities for authorizing disposal of records shall be vested with the delegated officers at branches./ offices as mentioned under para 10.5 of disposal of records

12.2 **Chief/Senior Managers**

Chief/ Senior Managers at RO/ ZO/ CO shall be responsible for the implementation of this policy in their respective units i.e. Central Office, Zonal Office and Regional Office/ Departments/Sections/Cell under the guidance of Delegated officers for assisting the delegated offices.. Chief/Senior Managers shall lead by example and shall themselves maintain good record keeping and record management services. Chief/Senior Manager shall ensure that all staff is made aware of record keeping and also towards their responsibilities and obligations for record management.

12.3 **Record Managers**

Following Officers shall be Record Managers at different locations:-

Sr.No	Type of Branch/ Office	Officer designated as Record Manager
1	Small/ Medium/ Large Branches	Branch Manager
2	VLB/ELB/ MCB/ CFB/ARB/ SAM Branches	Manager (Recovery/ Credit/ Operations)
3	Regional Office	Manager/Asst Manager (OPR/All depts.)
4	Zonal Office	Manager / Senior Manager (OPR/All depts.)
5	Central Office	Manager/ Senior Manager (all Central Office Departments/ Respective Sections/ Cell/ Divisions)

12.3.1 The Record Manager shall be responsible for:-

- The implementation of this policy
- Staff awareness regarding the policy
- The management of all record according to the record keeping policy
- Adherence to the retention periods as decided & conveyed by the Committee taking into account the functional, legal and historical need of the Bank to maintain record of transactions.

12.3.2 The Record Managers shall ensure that all the record created and received by Bank is classified according to the approved file plan and that a written disposal authority for them before disposal.

12.3.3 The Record Manager would ensure that unauthorized person(s) shall not have access to Bank's record. As and when any file/ document from record room is requisitioned, it shall be ensure that requisition slip is signed by authorized person. The Daftary should deliver the same only on written requisitions/ instruction of Branch Manager/ Department in-Charge.

12.3.4 In case of requisitioning of any voucher, the whole bunch of vouchers shall be delivered and entered in Record Movement Register.

12.3.5 If any paper or document is taken out from some file, substitution card or photocopy of such paper or document shall be kept on record with proper remark as to where original paper or document has been kept/ sent. It shall also be recorded on the Record movement register and ensured that the same is returned.

12.3.6 Even after the records have gone to the RSC, the ownership will continue to be that of the Branch/ Dept. The BMs/Departmental Heads are required to submit an Annual Certificate stating that the Record management Policy has been adhered to. Any violation of the policy will render the individual liable for disciplinary action.

12.3.7 **Closure and Merger:** In case of closure or merger of branches, the assistance of the Service Provider will be sought to update the database and also the record available with the branches. The 'Ownership' of the records will continue to be with be that of the updated/new Dept/ Branch and all concerned including the RO/ZOs will be informed. A record of annual check of correctness of quality and quantity will be done as mentioned above.

12.4 **Chief Public Information Officer**

12.4.1 The Chief Information Officer is responsible for approval of request for information in terms of the Access to Information Act.

12.4.2 The Chief Information Officer shall inform the record manager if a request for information necessitates a disposal hold to be placed on record that are due for disposal.

12.5 **Information Technology Manager**

- An official designated for the purpose posted at CO/ ZO/ RO or any other designated office shall be responsible for day-to-day maintenance of electronic systems that stores record.
- Work in conjunction with the record manager to ensure that record is properly managed, protected and appropriately preserved so long as required for business, legal and long term preservation purposes.
- Shall ensure that appropriate systems technical manuals and systems procedures manuals are designed for each electronic system that manages and stores record.
- Shall ensure that all electronic systems capture appropriate system generated metadata and audit trail data for all electronic record to ensure that authentic and reliable record is maintained.
- Shall ensure that electronic record in all electronic systems remains accessible by migrating them to new hardware and software platforms when there is a danger of technology obsolescence including media and format obsolescence.
- Shall ensure that all data, metadata, audit trail data, operating systems and application soft wares have back-up on a daily, weekly and monthly basis to enable the recovery of authentic, reliable and accessible record to have business continuity after a disaster.
- Shall ensure that back-ups are stored in a secured off-site environment.
- Shall ensure that systems that manage and store record are virus free.

12.6 **Security Manager**

The Security manager shall be responsible for the physical security of all record to prevent theft, sabotage, loss due to natural or any other reason/factor. Details regarding the specific responsibilities of the security manager shall be detailed in the information security policy.

12.7 **Head, Legal Department**

The Head of the Legal Department shall be responsible for keeping the Record Managers updated about developments in the legal and statutory environment that may impact on the record keeping and record management practices of the Bank,

12.8 **Record Room Staff**

Daftaries are responsible for the physical management of the record in their care. Detailed responsibilities regarding the day-to-day management of the record in the Record Room shall be as per the duty- list of Daftary issued by HRD.

12.9 **Staff**

12.9.1 Every staff member shall create record of transactions while conducting official business.

12.9.2 Every staff member shall manage the record efficiently and effectively by:

Allocating reference numbers and subjects to paper-based and electronic record according to the file plan(inward or outward); Sending paper-based record to the Record Room(Daftary) for filing; Ensuring that record is destroyed/deleted only in accordance with the written disposal authority.

12.10 **Formation of Committee**

12.10.1 A Committee of General Managers shall be formed at Central Office, which shall review the policy annually. The **General Manager, PDOD** will be the Convener of Committee and shall comprise the following General Managers as its members:

- General Manager - HRD
- General Manager - Credit
- **Chief Risk Officer/ General Manager - RMD**
- General Manager - **PDOD** (Convener)
- General Manager – Business Support Department (BSD)
- General Manager - (Audit and Inspection)
- General Manager - IT

CPIO, DGM-Legal, Chief Information Security Officer, Chief Security Officer shall assist the Committee.

12.10.2 **Responsibilities of the Committee:** The Committee shall be responsible to review the following :-

- (i) Content of the policy and updates;
- (ii) Durability – safe keeping / protection from deterioration;
- (iii) Accessibility and inspections required;
- (iv) Security – safety against fire, damage, theft, protection from Unauthorized access;
- (v) Examine adoption of technology and outsourcing of Record Management taking into consideration risk and reputation Risk involved in the event of non-availability of record;
- (vi) Information Asset security;
- (vii) Reviewing & deciding the Retention Period.

13. **Training**

- 13.1 The Record Manager shall successfully complete record management training that would equip him/her for his /her duties.
- 13.2 The Record Manager shall identify such training courses that are relevant to the duties of the Record Room staff and shall ensure that the Record Room staff is trained appropriately.
- 13.3 The Record Manager shall ensure that all staff members are aware of the record management policies and shall conduct or arrange such training as is necessary for the staff to equip them for their record management duties.
- 13.4 The training may be conducted at ZSTC in all zones Record Management may be made part of the training program in relevant courses.

14. **Monitoring and review**

- 14.1 The record manager shall review the record keeping and record management practices of Bank on a regular basis and shall adapt them appropriately to ensure that they meet the business and service delivery requirements of Bank.
- 14.2 This policy shall be reviewed on a regular basis and shall be adapted appropriately to ensure that it meets the business and service delivery requirements of Bank.

15. Audit and Compliance :

15.1 Role of Concurrent Auditor

The facility and the documents should be available for inspection by the internal/external auditors of the Bank, as also by the RBI auditors or any one authorized by the Bank. The Service Provider shall provide working space and a PC, if required, at the outsourced location for carrying out audit at the facility whenever required. The periodicity for the audit by the respective ZAOs of the Zone shall be once in a year and that by the CA will be once in 6 months.

15.2 The Service Providers facilities will be visited by a team of officers from the ZO/RO prior to utilizing their services to ascertain suitability for storage. The Audit Team will carry out the audit of the Service Provider once in a year and the CA representative once in 6 months. Apart from the above, the Branch/Department of RO/ZO/CO utilizing the services of the Service Provider will also detail a representative to verify and tally the quality and quantity of records held with the Service Provider at least once a year. A record of the same will be maintained and will be checked during the audit of the Branch/Department.

15.3 The vendor certifies compliance to the terms of the RFP and also enters into an agreement with our Bank as a token of acceptance of the terms mentioned therein. The fitness of quality and quantity of records is ascertained through the audit checks and the checks by the Branch/Dept. The records to this effect are preserved and maintained for production when desired by the checking authority. The reports provided by the vendor are as under:-

15.4 Third Party Audit Bank and/or RBI shall have the right to access to all books, records and information relevant to the outsourced activity of the service provider. Bank and /or RBI shall also have the right to conduct audit/s on the service provider by agents appointed to act on its behalf and to obtain copies of any audit or review reports and findings made on the service provider in conjunction with the services performed for the Bank. Service Provider agrees to allow persons authorized by it to access the bank's documents, records of transaction and other necessary information given to, stored or processed by the service provider and in the event these are not accessible to the bank within a reasonable time the bank would be liable to pay supervisory fees to RBI, in return same will be recoverable from the Service Provider.

This Policy be effective from the date of approval of Board.

Any revision in the Policy shall be approved the Board of Directors of the Bank.

ANNEXURE: I**Types of Record**

(All papers to be termed as a record should bear stamp and signature of the staff /official who handled it i.e. Cash receipt voucher should have cash receipt stamp and signature of receiving cashier, Inward Dak should bear Dak Received stamp with date and nothing of official authorized to receive the same.)

- 1.0 Vouchers
- 2.0 Letters, Statements, Returns etc.
- 3.0 Files containing correspondence.
 - i) Within Branch
 - ii) Inter Branch
 - iii) Within RO/ZO/CO
 - iv) With Customers
 - v) With sundry parties.
 - vi) With Govt/Quasi Govt. Depts./Bodies, Regulatory Authorities/Organizations, other Banks etc.
- 4.0 Audit Reports
 - i) Risk Based Internal Audit
 - ii) Special Report/100% Audit Report
 - iii) External Audit
 - iv) RBI Audit/Inspection
 - v) Inspection of any other nature
 - vi) Concurrent Audit
 - vii) Revenue Audit
 - viii) System Audit
 - ix) Management Audit
- 5.0 Applications for and sanctions of credit proposals and related documents
- 6.0 Control Returns
- 7.0 Statistical Returns.
- 8.0 Annual Closing Returns (P/L, B/S, LFCAR Tax Audit, External Audit)
- 9.0 Staff file and staff related files
- 10.0 Department wise / Subject wise Circular files
- 11.0 Telegrams/Telex/Fax/Email/Other Communications etc.
12. **Documents**
 - 12.1 Title deeds for properties (Purchase agreements) Insurance Policies, Lease Agreement, Purchase of Motor Vehicles, other Assets in the nature of Mechanical/ Electrical/ Electronic machines/equipment's and their Annual Maintenance Contracts.
 - 12.2 Documents executed by borrowers for credit facilities as also title deeds of their Properties deposited by way of Equitable Mortgage.
13. **Registers**
 - 13.1 Salary, O.T, Attendance, Bonus, PF/Gratuity, Pension, LFC/Medical Aid, Special Medical Bills etc, Staff Welfare –payments made under various schemes, various business / operational registers, Log books for vehicles, Office Order register/ files, Key Movement Register.

14. Ledgers and other Accounting books etc
- 15.1 Subsidiary {CD/HSS etc., Nominal Ledgers, Registers, Transfer books, Supplementary books, Summary books, Extract books, Cash books, General Ledger, GL Balance Book, Payment and Receipt Registers, OCC/BP/Collections Registers, Pay – slip issue Register, Cash Balance books, DD/MT/TT Registers and other accounting books etc.

ANNEXURE II

1. Vouchers

1.1 Duplicate vouchers

When voucher is lost and cannot be traced out, no duplicate thereof should be prepared without the Branch Managers sanction. The duplicate vouchers must be clearly marked as DUPLICATE in red ink and such duplicate voucher must invariably be prepared by Department-in-charge and be countersigned by the Branch Manager or in his absence second man i.e. Assistant Manager, Manager, Senior Manager etc. Details as to under what circumstances the original voucher was lost etc, must be mentioned on the back of the duplicate voucher and the same should be signed by the voucher passing officer and the Branch Manager or his absence second man i.e. Assistant Manager, Manager, Senior Manager etc.

2. Area covered – Methodology

Vouchers are the basic record in a branch/office. From the vouchers, the journals, ledgers, registers, transfer books, supplementary books, day books, cash books, general ledger etc. are written (prepared/generated). These vouchers/books are also required for the purpose of various types of audits/inspections carried out at the branches/offices. All these vouchers/books are, therefore, very important and they are required to be preserved property by the branches.

2.1 All the vouchers are to be stitched and batched daily after the routine work is over. Vouchers should be securely batched department wise / transaction wise and carefully preserved in such a way that no tampering with them is possible.

2.2 Each batch should be signed by the person who has stitched it after verifying the total number of vouchers with the individual concerned registers/books. The following information should be given prominently on the wrapper or each bundle.

No. of Debit vouchers_____ No. of Credit vouchers_____ Total _____
 Name of department: _____ Date _____
 Stitched by_____ (Signature)_____ (Name)
 Checked by_____ (Signature)_____ (Name)

2.3 All such batches relating to transactions on one particular date should be tied together between thick paper or cardboards and all the aforesaid information, including the signature of the person who stitched it should appear on the title of each bundle. Vouchers should be recorded in the “Register of Daily Vouchers”.

2.4 Specimen Register of Daily Vouchers

Date	Number of Vouchers	Total	Initials
	CD		
	OD/CC		
	HSS etc.		
	P/L, Nominal		
	& Others		

2.5 It will also be the duty of the Record Manager to ascertain from the supplementary books and cash book that the No. of vouchers relating to a particular date tally with the total No. of vouchers posted in these books on that date.

ANNEXURE III**FILE PLAN**

File No.	Departments
1	BUSINESS PROCESSING REENGINEERING (BPR) - BRANCH RATIONALISATION CELL, SYSTEMS & PROCEDURES
2	PENSION DEPARTMENT
3	CUSTOMER SERVICE
4	BUDGET, PERFORMANCE PLANNING & REVIEW (BPPR)
5	MANAGEMENT INFORMATION SYSTEM
6	STATISTICS CELL
7	CREDIT GUARANTEE
8	TRAVELLERS CHEQUES/GIFT CHEQUES
10	DEPARTMENT OF INFORMATION & TECHNOLOGY (DIT)
20	RISK MANAGEMENT DEPT (RMD)
21	CREDIT MONITORING & POLICY
22	CENTRAL STAFF DEPT. (CSD)
23	CREDIT INETREST RATES
24	REFINANCE
25	CREDIT AUTHORISATION SCHEME
26	TRANSPORT OPERATORS
27	INDUSTRIAL REHABILITATION
28	DW/IW/RO
29	SAM & RECOVERY
30	AGRICULTURE & RURAL DEVELOPMENT (ARD)
31	MSME & FINTECH
40	CREDIT
41	INDUSTRIAL RELATIONS & POLICY
43	STAFF ADMINISTRATION DEPT., (SAD)
44	RECRUITMENT & PROMOTION
45	DISCIPLINARY ACTION
46	PROVIDENT FUND
47	MANPOWER PLANNING & DEVELOPMENT
48	STAFF PENSION, GRATUITY AND RETIREMENTAL BENEFITS
50	HRD – (LEGAL, INDUSTRIAL RELATIONS & POLICY, R&P)
51	BOARD SECRETARIAT
52	SECURITY & TRANSPORT
53	SAFE DEPOSITE LOCKERS
60	BUSINESS SUPPORT DEPT (BSD)
61	BRANCH ACCOUNTS & CFO DEPT.
62	GENARAL ACCOUNT (B/S) DEPT.
63	MARKETING & NEW INITIATIVES
64	GOVERNMENT ACCOUNTS

RECORD MAINTENANCE POLICY OF THE BANK (UPDATED UPTO DEC-2022)

65	CURRENCY CHEST & CASH MANAGEMENT SERVICES
66	FRAUD INVESTIGATION CELL
70	AUDIT & INSPECTION DEPT (AID)
71	LOSS OF SECURITY ITEMS
72	DD/TT/LIMITS
80	INFORMATION & DATA ANALYTICS
81	VIGILANCE DEPARTMENT
82	RAJBHASHA VIBHAG
83	FUNDS MANAGEMENT DEPT.
84	LEGAL DEPARTMENT
85	TREASURY AND INTERNATIONAL BUSINESS
86	MERCHANT BANKING DIVISION
89	SYSTEMS & PROCEDURES DEPT.
90	SYNOPSIS OF CIRCULARS
91	KYC & AML CELL
92	COMPLIANCE DEPARTMENT