From, Indian Overseas Bank Central Office, General Administration Dept. Chennai 600 002.		To, All Domestic/Overseas Branches/Regional Offices/Other Offices in India. Circular No. MISC/201/ 2024-25 dated 20.03.2025

Document Handling and Data Retention Policy

We are pleased to inform that our Bank's Board on 18.02.2025 has approved new **Document Handling and Data Retention Policy** in line with the prevailing Statutory /Regulatory guidelines and applicable laws, which involves preservation of records pertaining to various verticals covering the entire Bank.

The Policy covers classification, storage, retrieval, and disposal of records pertaining to Branches and Administrative Offices. Guidelines and SOP for offsite record maintenance using outsourced agencies has been elaborated in the Policy.

Further, detailed guidelines has been put forth for Digitalization of Physical records using Electronic Record Management system for the purpose of Archiving/Storing the records and the procedures to be followed in preserving, retaining, archiving, and purging of the Digital Data.

This policy is valid for three years from the date of approval by the Board i.e till 29.02.2028.

Any further Circulars/ any changes suggested by RBI / Other regulatory authorities during the currency of the said Policy, will automatically form part of the Policy.

All are advised to take note of the contents of the policy for their guidance and ensure compliance.

AMIT KUMAR
Digitally signed by AMIT KUMAR
Date: 2025.03.20 16:49:45 +05'30'

AMIT KUMAR
(DEPUTY GENERAL MANAGER)

Document Handling and Data Retention Policy

Approved on 18.02.2025

Valid upto 29.02.2028

Indian Overseas Bank,

General Admin. Department,

Central Office

Index

PART A – DOCUMENT HANDLING AND RETENTION (PHYSICAL RECORDS/DOCUMENTS)

PART B – DATA RETENTION (HANDLING & RETENTION OF DIGITAL DATA)

PART C – PRESERVATION PERIOD OF RECORDS - FOR DEPARTMENTS AT CENTRAL OFFICE

1. PREAMBLE:

Bank, as a financial intermediary, dealing in various types of financial transactions has obligations under law to maintain, handle and preserve records either permanently or for certain specified period. Applicable law in this regard is contained in Bankers Book Evidence Act. 1891, RBI Act 1934, Companies Act, 1956/2013, Banking Companies (Period of preservation of records) Rules 1985, Prevention of Money Laundering (Maintenance of Record) Rules, 2005, etc.

All records in offices are required to be taken proper care of so that they are preserved for the periods as required under law. It is essential to have proper storage, retrieval and disposal controls of such records as well, as the bank deals day-in-day-out with high-risk security documents. Records are to be preserved carefully, so that they are available for any reference in future. Therefore, handling of documents/ records assumes great significance in banking operations.

BACKGROUND:

- Our Bank had a **Records Maintenance Policy** (Systems and Procedures) in the year 2003, it had classified preservation of physical records based on legal, regulatory, and other requirements of the Bank.
- With the enactment of Right to Information Act 2005, during 2013, the policy was renamed as **Document Handling and Retention Policy**. As per the policy the period of conservation of Bank's physical records was fixed for a period ranging from 1 to 20 years or PERMANENTLY. The policy was last renewed for a period of 3 years from the year 2020 to 2023.
- The vast technological changes in the Banking Industry necessitated retention / preservation of huge electronic data. Hence, retention / preservation of electronic data also assumes greater significance and accordingly the **Document Handling and Retention Policy** has to be revised and renamed as **Document Handling and Data Retention Policy,** apart from Physical records the new policy lays the guidelines for handling and retention of digital / electronic data.

2. OBJECTIVE:

- To formulate guidelines in consonance with the law to Preserve, retrieve, withdraw, redeposit and dispose records in an efficient, secured and cost-effective manner.
- To introduce, classify & manage record preservation schedule at branches/offices of the Bank in accordance with the procedure laid down for custody, upkeep, inspection, retention, and destruction of records.
- To ensure that the Bank's business is adequately documented and managed in accordance with best practices.
- To perceive and mitigate the risks on record storage and maintenance.
- To help the employees 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.

3. SCOPE:

The scope of the policy is to provide a set of guidelines and procedures to classify, store, retrieve and dispose of the documents related to financial transactions, administrative records, registers and documents in physical and electronic at different level such as Branches, Regional offices, Zonal Audit Offices and Central office. **Part A** of this policy document is about handling/retention of physical records whereas **Part B** is about handling/retention of digitized data. These guidelines are applicable to all modes of storage including electronic mode, to be preserved that is to say:

a. Records to be preserved permanently

b. Records to be preserved for not less than10 years

c. Records to be preserved for not less than 8 years

d. Records to be preserved for not less than 5 years

e. Records to be preserved for not less than 3 years

f. Records to be preserved in respect of Govt. Transactions

4. PREVAILING STATUTORY / REGULATORY GUIDELINES AND LAWS APPLICABLE:

a. Banking Regulations Act, 1949;

b. Companies Act, 1956/2013;

c. Income Tax Act, 1961;

d. Indian Evidence Act, 1812;

e. Banking Companies (Period of Preservation of Records) Rules, 1985;

f. Bankers Books Evidence Act, 1891;

g. RBI Act, 1934;

h. Information Technology Act, 2000;

i. Right to Information Act, 2005;

j. Prevention of Money Laundering Act, 2002;

k. Regulation 9 of SEBI (Listing Obligations and Disclosures Requirements), Regulation

l. IRDAI Regulation 2020 for information required for investigations.

m. GOI Guidelines on E-Waste Management (Storage Media)

OTHER REFERNCES:

- Bank Information Security Policy
- Meity/CERTIN Directions 70B dated: 28.04.2022
- Meity/CERTIN Security Guideline CISG – 2008-01 dated31.12.2008
- [SEBI Cyber Security & Cyber Resilience framework for Stock Brokers / Depository Participants dated 03.12.2018]
- Digital Personal Data Protection Act 2023
- RBI Master Directions for KYC AML
- Banking Companies rules for preservation of Records 1985
- Information Technology Act 2000(Amendment 2008)
- Information Technology Rules 2000 (CA)
- Digital Personal Data Protection Act 2023
- UIDAI, Aadhar Act 2016

5. DOCUMENTS/RECORDS ITS TYPES AND SIGNIFICANCE:

A. Physical Records:

For the purpose of 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.

B. Electronic Records / Digitized Records:

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.

Bank creates documents/records/data through internal employees" activities and from external transactions and correspondence those documents/record/data should be considered as an asset and it enables bank:

a) To find the right information easily, comprehensively & completely and to perform its functions successfully and efficiently in an accountable manner.

b) To support the business, legal and accountability requirements of the Bank.

d) To ensure the smooth conduct of business in an orderly, efficient, and accountable manner.

e) To ensure adherence to Statutory/regulatory requirements.

f) To ensure the consistent delivery of services and to provide continuity in the event of a disaster.

g) To support and document policy formation and administrative decision-making

h) To protect the interests of the bank and the rights of employees, clients, and present and future stakeholders.

i) To support and document the Bank's activities, development, and achievements.

6. MODE OF RETENTION/ PRESERVATION:

The documents specified in Annexures to this Policy, shall be retained/ preserved, in:

- Physical form (Hard Copy) and/or
- Electronic/ digital or digitized forms/scanned copy (Soft Copy)
- or in Both the forms

a) The preservation of documents should be such as to ensure that there is no tampering, alteration, destruction or anything which endangers the content, authenticity, utility or accessibility of the Documents.

b) The preserved documents must be accessible at all reasonable times. Access may be controlled by Authorized Officer, to ensure integrity of the documents and to prohibit unauthorized access.

c). Every official of the Bank shall be responsible to maintain the records as per the duties and responsibilities assigned to him/her from time to time vis-à-vis the importance and confidentiality of the papers/ documents handled while discharging duties.

d). The records shall be maintained simultaneously with the completion of transaction or completion of a given task.

PART A – DOCUMENT HANDLING AND RETENTION (PHYSICAL RECORDS/DOCUMENTS)

7. PHYSICAL RECORDS /DOCUMENTS

Physical record is either in original or copies of correspondence and Business forms which include account opening forms & supporting documents, vouchers, registers, ledgers, statements, correspondence, agreements, invoices, licenses, certificates, photographs, films, and other kinds of documents.

7.1. Storage:

The Branches are to hold the records normally in the Branch premises itself. Where for some valid reasons viz., space constraints, high rentals, multi-storied buildings etc., if it is necessary to hold records at a different location, Branches shall do so with the prior approval of Regional Office.

In this regard, Regional Offices can explore the possibility of having common Off-Site record rooms for City Branches, in sub-urban areas / peripheral areas, where premises rent would be cheaper. This would bring down the cost of holding records considerably.

7.2 Off-Site Records Rooms:

- Regional Office shall identify and approve such Off-site Record Rooms, to keep all old records (except Security Documents & Title Deeds) of Branches (in that Region). It shall however be noted that the records of each Branch are kept segregated and kept separately within the same off-site record room.
- All records, older than three years, may be sent to such identified place for storage.
- Branches to keep proper record of the documents sent to such off- site record rooms for preservation.
- It is to be noted that all those documents requiring dual control viz., Security Documents and title deeds, shall be kept in Branch only and not in off-site record rooms.

The risks involved in holding physical records, shall be mitigated by ensuring the following:

a) Records shall be kept neatly and methodically in conditions that are secure and clean with low risk of damage.

b) Each register and files being conspicuously numbered and dated for easy reference.

c) A Record Register shall be maintained in the Branches for each description of books and files. Separate page / sheet shall be used for each type of registers / ledgers / files and their retention period recorded thereon.

d) If the records are maintained in approved places other than the Branch, then address of the location where the records are held should be clearly mentioned in the Record Register.

e) Old records shall be placed in charge of Record Keeper who should be held responsible for the records lodged at Branches / Offices / Off-Site Record Rooms.

f) All records kept for preservation inside the Branch or with off-site record room, shall be given serial references / index number based on the number of years of storage. Such reference shall be only with the authentication of authorized official nominated for the Branch / Office etc.

g) Manager / Deputy Manager from Branches or a designated Official from Administrative Offices shall inspect the record room once a month and ensure that the records are properly maintained. The Record Register and Record Requisition Register should be verified.

h) The electrical wiring inside the record room shall be properly concealed in casing, so as not to have exposed wiring. No adhoc / bare electric connection is to be permitted inside the record room. The record rooms shall have detachable plug and socket arrangement for power connection, to minimize the risk of fire due to electric short-circuit, during non-office hours.

i) Fire extinguishers (ABC - Dry Powder type) shall be available and fixed prominently outside the record room. The powder shall be refilled periodically, before its expiry.

Records are to be preserved for the prescribed period in branches/offices or off-site storeroom after proper indexing. The off-site storeroom should be under the control of General Administration Department, Regional Office, if the record pertains to Branches / Regional Office. In the case of old records pertaining to Central Office, the storeroom shall be under the control of authorized officer in charge of the concerned department of Central Office.

7.3 Retrieval of Old Records / Data / Archives:

a) Retrieval of records from the Record room shall be only in the presence of branch custodians (Branch Head or any authorized official of the branch)

b) For retrieval of Records, from an off-site record room approved by Regional Office, Branch shall ensure the following:

- Make a request to Regional Office with clear purpose and proper authentication, with a copy marked to the record room. Request to be considered for processing by the concerned Office within 24 hours.
- The request is registered in the Records Requisition Register, clearly mentioning the details of items taken out with the initials of the receiver, date of re-deposit etc. The above shall have to be duly authenticated by the authorized official.

c) No record shall be allowed to go out of custodian without being entered and receipted by the employee under due authority requiring it, in the Records Requisition Register.

d) It shall be ensured that all such records are promptly returned and duly authenticated with date in the Register by the Record Keeper in charge of Records.

e) To avoid tampering:

- Records are to be handed over only to Staff duly authorized by an Officer of the Bank.
- On receiving back, the Record must be physically verified the total number of vouchers again and tally with the totals recorded in the voucher register / cover sheet of the voucher bundle.

f) In all cases, where records are to be taken possession by the Police / Governmental authorities, a written requisition must be taken and an acknowledgement obtained from the recipient in respect of the record to be taken possession of or delivered to, retaining copies of the records delivered.

g) It is the duty of the Branch to ensure that, items / documents which are all taken out from dual control are once again placed inside at the end of the day.

h) A separate register shall be maintained for listing and recording all books of accounts, files and registers in current use with the respective current numbers and separate register for those items retained for preservation. The register shall be complete, recorded with updates, proper labeling of each of the items, placed in the records, will facilitate easy location and handling of items in old records.

7.4 Classification of Record Preservation:

- The retention period of information is an important aspect in the records life cycle. It identifies the duration of time for which the information should be maintained or "retained".
- Schedules of books and files, which are maintained manually, at ADMINISTRATIVE OFFICES (Central Office, Regional Offices etc.), with the period for which these must be retained on record, are furnished as **Annexure I** to this policy. Similarly, schedules of books and files, which are maintained manually, at Branches, with the period for which these must be retained on record, are furnished as **Annexure II** to this policy.
- The retention period specified in Annexures, in the case of a file, is to be reckoned from the year in which the file is closed (i.e., action thereon has been completed) and not necessarily from the year in which it is recorded.
- In the case of records other than files, e.g., registers, the prescribed retention period will be counted from the year in which it has ceased to be current.
- In exceptional cases, a record may be retained for a period longer than that specified in the schedule, if it has certain special features

or such a course is warranted by the peculiar needs of the department. In no case, however, will a record be retained for a period shorter than that prescribed in the schedule.

- If a record is required in connection with the disposal of another record, the former will not be weeded out until after all the issues raised in the latter have been finally decided, even though the retention period marked on the former may have expired in the meantime. In fact, the retention periods initially marked on such records should be consciously reviewed and, where necessary, revised suitably.

7.5 <u>RISK PROFILING/ CATEGORIZATION OF PHYSICAL RECORDS TO BE RETAINED:</u>

Various types of Records are retained by the Bank. Some of those Records are very crucial and important while a few of the Records may not be so crucial and important. Normally importance of any Record is associated with different factors like frequency of its requirement in relation to complaints, Court Cases, RTI Queries etc. Therefore, while the operational unit holding/retaining the Records, it should be categorized in three risk buckets viz, High Risk, Medium Risk and Low Risk depending on the nature of the Record. Accordingly, suitable priority to be assigned to various categories of Records while holding/preserving/retaining the same.

Broader guidelines regarding classification of records into High, Medium and Low Risk category is as below.

i) **High Risk Records** are the records / documents that are sensitive / confidential / secret, that pose a significant risk to the organization if they are misused, lost, damaged, or deleted permanently.

ii) **Medium Risk Records** are those records / documents not for disclosure to the public or external parties but generally available to the Bank employees and authorized non-employees, but those documents without which the operational performance would be compromised.

iii) **Low Risk Records** are those records that are available for public disclosure, the loss of which will cause slight inconvenience or difficulty in operational performance of function or activity area. Recovery from such consequences would be handled quickly without the need to divert resources from the core activity area. The records which do not bear much of risk factor in their safe keeping like System generated reports, various registers which are used on day-to-day basis in regular banking operations.

7.6 Protection Clause:

- During the currency of preservation, reasonable care is expected to be taken of all records. For the purpose, it is necessary that frequently the records must be kept sprayed with insecticides/pesticides or alike treatments to prevent occurrence of termites, silver fish, white ants or any other type of insect and consequent destruction of records.
- Neglecting the care of records may ultimately result in a regret as by law, it is necessary that due care must be taken of the records.
- Law does not afford any protection in respect of any negligence in the matter of preservation. The only protection available is in case of records destroyed by fire, water logging, flood, earthquake, or any other Act of God.
- Where such a circumstance comes about, a list must be made in respect of the items that are missing and an endorsement must be made on the register stating that the record Item No. are destroyed by fire, water logging, flooding, earthquake or any another act of God. Complete details should be provided. This is the only protection available in case of circumstance beyond human control.
- The insurance of the records stored off – site must be entered into by regional office concerned. The Regional office must 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.

7.7 Safe keeping and handling of important Security Instruments /Documents:

Items which form part of security items are:

a. All kinds of Deposit Receipt Books

b. Cheque Books

c. Loose leaf cheque books

d. Demand Draft

e. RBI/Other Bank's Cheque Books

f. Forms of Letter of Credit

g. All/any of the above on continuous stationery

h. Debit/Credit Cards

i. Ready Kits/PINs

j. Any other item of stationery involving risk and security aspects for the Bank.

- On receipt of any security items mentioned above from Printing & Stationery Department/ Printers/Suppliers, proper verification including physical verification, should be done by the authorized official of the branch, with reference to indents placed, the forwarding letters, packing lists, etc.
- Noting of having checked/counter-checked be made on the cover of each book and be signed by the official. Receipted challans should be immediately sent to the concerned department to facilitate payment of bills.
- After recording the receipt of such items in the relevant register/books, the authorized branch official will ensure and authenticate that the stock of such items is received correctly intact in chronological order and that nothing is missing from the stock sent.
- In case any item/quantity is missing from the stock indented/sent, the authorized branch official will immediately bring the fact to the notice of the Branch Manager and take prompt steps to report the position to the concerned Regional Office/ Department/ Printers/ Suppliers. Prompt action in transmitting the information of loss of security items is a vital step in prevention of frauds.

- All valuable forms such as Cheque books/Draft Books/Deposit Receipt Books/Loose Leaf Cheque books, ATM/Debit/Credit Cards and other items listed above, should remain under Lock and Key, preferably in steel almirahs in the Joint Custody of Two Officers, one of whom must be Branch Manager/Deputy Branch Manager or Senior Clerk and it should be controlled through a separate register.
- Whenever any item is taken out for day-to-day use the need for the same should be established and only then, the date when such item is taken out for use and the quantity should be recorded in the relevant registers/book. Acknowledgement from the official to whom the item is delivered is to be obtained.
- The authorized branch official will arrange to keep such Security Stationery/Documents/ Valuable Forms and other items listed above in safe custody in a proper order and report the position to the Branch Manager/Deputy Branch Manager/Senior Clerk.
- The Branch Manager/ Deputy Branch Manager/Senior Clerk will ensure that these items are always under proper control and adequate balance of stock is maintained properly.
- The clerk/official with whom the DD books/Deposit receipts etc. remain while in use during the day shall be responsible for proper safe custody of these forms/security items during the working hours. If he/she leaves the counter, during working hours, proper arrangements should be made to keep watch over such forms/security items. This equally applies and more so, in respect of security items printed on continuous stationery.
- Branches are required to maintain a record/register of various important items as listed above, the stock recorded therein should, therefore, tally with the stock lying under their control. However, if no physical verification is done periodically and if any book is removed unauthorized by anyone, the incident of loss of such book would not come to light immediately. With a view to introducing an element of check in such occurrences, branches as well as inspecting officials should undertake physical verification of security items and submit certificate in the following manner:

A. Physical verification of security items by branches:

All branches should undertake physical verification of stock of security items on quarterly basis and send a certificate in the following proforma to their Regional Office within seven days from the end of the quarter:

Format of Quarterly Certificate

(To be submitted by the Branch to Regional Office)

From _____Branch	To, The Regional Head Regional Office _____
Ref No:	Date:

Subject: Certificate of verification of Safekeeping of Security Items for the quarter ended_____

"We certify that we have undertaken physical verification of stock of all security items as of _____and confirm that the stock of these items is in agreement with the stock recorded in the relevant books. No book/leaf of any security item is missing. We also confirm that all redundant/unusable stocks of security items such as old Demand Draft leaves/non-CTS cheque books etc. have been destroyed and there is no unusable/redundant stock of any printed security item lying at the Branch."

Branch Second line Branch Head

- In all cases of loss/theft of items of stationery involving security risks, accountability is to be fixed immediately irrespective of the actual loss incurred by the Bank. In other words, even in case of failed attempt of fraud, matter is to be viewed from the accountability point of view.
- Even the officials in Regional Office who are entrusted to monitor submission of quarterly certificate from branches as mentioned above shall be held accountable for any lapses on their part in obtaining the certificate or in respect of any discrepancies therein.
- Stock of unusable / redundant / discontinued stationery items including security items should be destroyed and confirmed to the Controlling Offices immediately on receipt of such instructions from Central Office, from time to time, in order to prevent such old stocks being put to misuse.

7.8 Security Documents and Title Deeds etc.:

- Branches obtain loan agreements, Security Documents; take deposit of title deeds of Properties Mortgaged to the Bank etc. at the time of loan sanctioning
- These are entered in safe in safe out register at the Branches and are kept in safe custody under dual control.
- It is clarified that these documents shall continue to be preserved at the Branches under dual control till duly disposed of.
- In case originals of the agreements, security documents and the title deeds are required to be produced in the court in any litigation, then the documents taken out shall be entered in the "Safe in Safe out" register under the initials of joint holders.
- Further name and designation of the persons who have taken out the documents should be entered in the register.
- It is clarified that after handing over the documents to the Advocates, proper acknowledgement of receipt shall be obtained, and such acknowledgement shall be kept pasted in the safe custody register at the relevant page.
- It is further clarified that the security documents, title deeds etc. shall not be sent to the old records. These documents should be kept in a safe and secure manner as the Bank is under an obligation to return the original title deeds after closure of outstanding loans in full.

Provision/Clause regarding "Handing Over/ Taking Over" charge of Branch by Transferee Branch head and New Incoming Branch Head:

- It may be noted that the new incumbent shall effectively take over the charge from his predecessor only after ensuring that the records/documents/ registers in respect of transaction of the branch/office are properly maintained and safely preserved in the branch/ office. Also the documents related to any court cases, which are under the investigation of probe agencies such as CBI / FIU should be thoroughly verified at the time of taking over.

8. Removal and Disposal of Old Records:

As time passes, the period for preservation lapses and such items are permitted to be withdrawn from the records and disposed, appropriately. If the process of elimination of records is systematically done every year, the total quantum of records for disposal are not sizeable and will avoid accumulation and demand on space.

8.1 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.

Sl .No	Branch/ Office	Sanctioning Authority for disposal of Records
01	All Branches upto Scale-IV (Small, Medium & Large)	Second line of respective ROs
02	All Branches above Scale – IV	Branch Manager
03	Regional offices	Regional Head
04	Zonal Audit Offices	Head of the office
05	Central Office	GM / HOD of the concerned Department
06	Other Offices	Head of the office
07	Staff Training College/ STCs	Principal of Staff Training College/Concerned Regional office of the STC attached with

8.2 Action to be taken at the Regional Level:

- Branches shall prepare a detailed list to including file details, documents detail etc. which should be forwarded to Regional office. As soon as the list is submitted by the branch for destruction/ disposal of records, it must be scrutinized at the Regional Office by an officer duly authorized not below the rank of Scale IV for the same and permission to be accorded to the branch after due scrutiny of the list submitted by the branch.
- After due scrutiny, Regional Office may endorse permission for destruction/ disposal by the branch. After a reasonable time from the date of such permission accorded to the branch, a reminder must be sent to the branch as to whether the records permitted to be destroyed are destroyed or not and to call from the branch a certificate to that effect.
- 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 2nd line functionary at ROs.
- For the purpose of enabling the Regional Offices to know the position at any time, a register is to be maintained in a specified format which serves as a Watch Register to ensure compliance of the instructions given to the branches for elimination of stale records.

For destruction of records upon expiry of the period prescribed in this policy statement, control measures including (but not limited to) the following, shall be adhered to:

1) Authorization and approval prior to destruction.

2) Branches / Offices of the Bank shall maintain record in the registers giving details of the documents in paper / other form destroyed, along with the date and means of destructions.

- The destruction shall be by means of shredding and disposing the same if the quantity is too small for sale or disposal to wastepaper dealers.
- Regional Offices are required to call for rates from two or three wastepaper dealers locally and dispose of the records duly

shredding / tearing into pieces in the presence of the Head of the Branch or a person designated by him / her for the purpose.

- Regional Offices can arrange for sale of old records by arranging common purchaser for the Region. After disposal of the records, a certificate must be sent to the concerned Regional Office about having destroyed the old records in pre-defined format.
- The procedure for elimination of records prescribed for Branches as above is applicable to Regional Offices also, permission from General Administration Department, Central Office should be obtained for elimination of old records pertaining to them.
- The process of elimination of records can be conveniently taken up by the Branches/ Regional offices/Central Offices, preferably in the month of June, when relatively other works are not heavy.

Method of shredding can also be used as it is safer and has realizable value too.

a) All records, Books and Files shall be destroyed after the expiry of the respective retention period provided; they are not required for any special reason.

b) Wherever investigations / litigations are pending, records to the same such as Registers, Vouchers etc. should be preserved beyond the stipulated period, till such time the investigation / litigation is over, and the destruction of records is to be approved by the Regional Office / Central Office.

c) Prior permission from Regional Office / Central Office to be obtained to dispose of / destroy any records before the expiry of stipulated retention period or where a particular record is not listed.

d) Papers in all correspondence files both inward and outward should be scrutinized and only such of the papers which are not of any importance may be destroyed. Papers which are of a permanent nature should be filed again in a file to be marked "File of Permanent Nature" for the years from _____to _____.

e) Subject to the aforesaid conditions and keeping in view the time limits prescribed for preservation referred to above, annually a list of records proposed to be destroyed should be drawn up as per the organizational setup of the Bank and shall be submitted accordingly to

the controlling Office(s) concerned, for approval. Such list shall be forwarded to the office concerned on or before 30th June every year. The said list to be drawn up and should be signed by Officer(s) concerned.

8.3 Written Off Loan Accounts:

i. Written Off Loan Accounts for which CGTMSE / CGTSSI / CGFMU claims have already been settled and adjusted to the loan accounts, the loan papers, files, registers etc., be maintained for a period of 5 years from the date of closure and later eliminated, provided there is no chance of recovery.

ii. Written Off Loan Accounts for which, claims have been lodged with CGTMSE / CGTSSI / CGFMU but are pending for settlement, the loan papers, files, registers etc., be maintained for a period of 5 years from the date of settlement of claim.

iii. Non- CGTMSE / CGTSSI / CGFMU loans (General Category) which, have been fully written off, the loan papers, files and registers for these loan accounts, be maintained for a period of 5 years from the date of closure and later eliminated, provided there is no chance of recovery.

iv. Written Off Loan Accounts for which CGTMSE / CGTSSI / CGFMU claims have already been settled and adjusted to the loan accounts, the loan papers, files, registers etc., be maintained for a period of not less than 5 years from the date of closure of account of current calendar year.

v. Written Off Loan Accounts for which, claims have been lodged with CGTMSE / CGTSSI / CGFMU but are pending for settlement, the loan papers, files, registers, etc., be maintained for a period of not less than 5 years from the date of closure settlement of the claim of the current calendar year or date of closure whichever is later.

vi. Non - CGTMSE / CGTSSI / CGFMU loans (General Category), which have been fully written off, the loan papers, files and registers for these loan accounts be maintained for a period of not less than 5 years from the date of closure of the account, in the current calendar year.

vii. Any Written Off Loan Account in which fraud has been detected or investigation is in progress and staff accountability is ascribed, in

such cases prior permission to be obtained from the General Manager, FRMC for elimination of records irrespective of the period since they are maintained.

8.4 Government Transactions:

The records pertaining to Government transactions should be destroyed only after getting prior permission from Government Accounts, Central Office.

8.5 Disposal of all other Items including Stationery, Security Items:

All the unusable / redundant / discontinued stationery items such as Vouchers, Withdrawal slips, Cash Receipt slips, **Non – CTS cheque books** etc. and all other non – security stationery items shall be shredded / destroyed by fire in at branch level, in the presence of Officer as per the delegated powers. Such record may also be sold to bonafide paper manufacturers as approved by Regional Offices after obtaining an undertaking from them to turn the material into pulp at once and not to allow any to pass to other hands.

For disposal of other redundant items such as credit cards, debit cards, pre – paid cards, gift cards etc. and security items like cheque books, banker 's cheque etc. of the closed / merged branches, the branches have to take up with the Regional offices and Regional offices should get approval from the relevant Departments at Central Office, after approval from the relevant dept the same shall be disposed.

9. Miscellaneous

Inspection and Follow-up:

If in the Inspection Report, a mention is made about the storage of records and the irregularities there in, the inspection Dept. will send a copy of the inspection report to the Regional Office for follow-up actions. Such irregularities will have to be taken up with the Branch by the Regional Office and it must be ensured that the Branch rectifies the irregularities within a reasonable time and reports to the Regional Office.

Interpretation:

This Policy has been framed to comply with extant laws of the land, governing the Bank. If under any circumstances where the terms of this policy differ from any existing or newly enacted law, rule, regulation or standard governing the Bank, the law, rule, regulation or standard will take precedence over this policy.

Review of the Policy:

The policy shall be reviewed annually in tune with the regulatory guidelines / internal requirements or as and when necessary. The Policy to be modified in tune with regulatory requirements, from time to time.

Any significant changes suggested by RBI/other regulatory authorities during the currency of the said policy, will automatically form part of the policy and the same may be permitted after approval from MD & CEO.

Validity of the Policy: The policy is valid for 3 years and the policy shall be reviewed once in a year. MD & CEO is empowered to extend the validity of the policy for a further period of six months in case of exigencies.

10. OFFSITE RECORD MAINTENANCE USING OUTSOURCED AGENCY:

- In case banks record is to be warehoused in a facility managed by an outsourced agency, the bank must ensure that all requirements as regards safety, security and availability are met fully. Facility should be subject to security under IS Audit and should be available for RBI inspection.
- In considering an outsourcing arrangement, appropriate due diligence should be performed to assess the capability of the service provider to comply with obligations of the Bank. 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 whether their standards of performance including in 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.
- Due diligence should involve an evaluation of all available information about the service provider, including but not limited to:
  - ✓ 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.

10.1 Roles and Responsibilities of Service Provider:

(i) Collection

The Service Provider will visit different branches/offices of the bank for collection of record/documents which are not used in day-to- day business but to be preserved as per the policy in physical form i.e. files, bound vouchers bundles, registers, ledgers etc. for storage at Record Storage Centre (RSC) in a time bound program 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 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. The list of inventories will be treated as a Branch document and shall be kept in safe custody, preferably in a fireproof safe.

(ii) 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 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 inventories. Bar coding should be tamper/waterproof.

(iii) Transport

The Service Provider will arrange lifting of 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.

(iv) 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 regulations. 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.

- 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. Periodic inspection by RO or CO officials or by any 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 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.

10.2 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 e-mails or letters from the authorized officials of the bank. Retrieval shall mean delivery to the bank's premises at different locations.
- 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.

Turn-Around-Time (TAT):

Nature of Retrievals	Turn-Around-Time (TAT)
Ordinary Retrievals	All requests by 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 e-mail received by 12.00 noon will be delivered on the same day to local branches/courier.
Bulk / Project Retrievals	As communicated by the bank at the time of assigning the task (with mutual consent)

Retention of Records:

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

10.3 Destruction/Permanent Retrieval of 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 Bank's Policy and inform the concerned branch/office and seek their written consent for destruction.
- ✓ Unless there are instructions to the contrary, 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 obsolete records to chemical furnace or paper mill, for burning or converting into pulp.

10.4 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 law dept 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 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, records, 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.

10.5 Confidentiality and Security:

- 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.

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

10.6 Monitoring and Control of Outsourced Activities:

(i) 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.

(ii) 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.

(iii) 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.

(iv) 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.

(v) The Service Providers facilities will be visited by a team of officers from the CO/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. Apart from the above, the

Branch/RO/Department of 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.

(vi) The vendor certifies compliance to the terms of the RFP and 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:-

Reports:

a) 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.

b) Total number and details of the cartons with size containing records of the bank being stored at RSC.

c) Total number and details of the bank's cartons/records retrieved (delivered) during a period.

d) Total number and details of the bank's cartons/records returned by the Bank.

e) Total number and details of the bank's cartons/records destroyed.

Insurance:

Stored Material is not insured by Company as ownership of the Records lies with the Customer. The insurance of the records stored must be entered into by regional office concerned. The Regional office must 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.

Penalties:

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

Ordinary Retrievals:

Applicable Condition	**Applicable Penalty**
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 themonth

Urgent Retrievals

Applicable Condition	**Applicable Penalty**
Retrievals which are not adhered to in 1 day TAT-will beconsidered as Ordinary Retrieval	As above.

10.7 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.

11. DIGITILIZATION OF PHYSICAL RECORDS – ELECTRONIC RECORD MANAGEMENT SYSTEM

- Digitization of records is the most economical, effective, and durable way to maintain records. It not only helps to free the space, but also helps to maintain the records effectively for longer duration and easier reproduction, in case of reference. Digitization is the process to convert physical documents/ copies / records (viz. memos, memorandums, notes, office orders, letters, minutes of meetings, correspondence, etc.) into electronic / digital format.
- **Document Management System (DMS)** is a system that electronically manages the flow of documents particularly receiving and releasing. This system includes features such as bar graphs for tracking records, etc. It should be noted that the DMS is not the same as an Electronic Records Management System which has broader coverage and functionality
- **Electronic Records Management System (ERMS)** refers to an automated system used to manage the creation, use, maintenance, and disposition of electronically created records for the purposes of providing evidence of business activities.
- 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** or **Centralized Document Archival Centre**
- While shifting to electronic records is a necessity, Bank has the option of retaining hybrid records management systems involving both paper and electronic records. It is foreseen that such hybrid systems will be the norm up to the near future.
- Therefore, offices/branches should initiate all possible and feasible steps to digitize the records which are maintained in physical form to reduce and save the space.

11.1 CREATION AND CAPTURE OF ELECTRONIC RECORDS

This section discusses the first of the three phases of a record's life cycle.

A. Creation

Every record goes through three phases; a record is created, it is maintained and used, and it undergoes the disposition process. To facilitate later phases of the life cycle, records creation must be managed effectively. Records created must adequately and accurately reflect bank's policies, transactions, decisions, procedures, functions, and activities. There should be sufficient metadata added to provide the needed context of the records. Titles of records are assigned at the time of creation.

- **Naming Convention** provides a set of rules to assign names to records in a consistent manner. Naming conventions should be established to facilitate retrieval and reliable understanding of business activities in the ERMS environment. Establishing a uniform file naming convention based on the agency-wide functional/ operational requirements ensures that all electronic records in a file plan are equally retrievable by all users in the shortest possible time.
- **Version Control.** The Bank must establish procedures that will identify and differentiate an official record's earlier/ multiple versions to avoid confusion regarding which record is final/ official.
- **Digital Signature**. The digital signature is used to establish a person's credentials during transactions. A digital signature is an electronic signature that is used to authenticate the identity of the sender of a message or the signatory of a document as well as to ensure that the content of a document or message is secured from unauthorized changes by a password. A digital signature may only be applied to a document by a password holder.

For permanent records, the printed name of the digital signer, as well as the date when the signature was executed should be included in the electronic display and the hardcopy of the electronic record. This will preserve the name of the signer as part of the electronic record. A digital signature is deemed equivalent to a handwritten signature. For this reason, the signature owner must protect her /his password so that it cannot be used by others. Even when a digital signature is used by others, the original owner is liable for whatever her /his digital signature authorizes.

B. Capture

- Capturing documents in the ERMS as records is mandatory. Records in the ERMS cannot be deleted or altered without proper authorization and audit trail.
- Document Management Systems (DMS} should not be used to capture and store records in place of an ERMS. A DMS is not designed for recordkeeping purposes but to simply manage documents. A DMS allows documents to have many versions, to be modified, and to be deleted by their owners. Fully operational ERMS should include all the functions of a DMS.
- Paper records should be captured in an ERMS by digitization or conversion to digital format through scanning to prevent loss of data.
- An ERMS should capture complete records. The structure and contextual information necessary to document an official activity or transaction must be captured together with the content of the record. Capture record keeping metadata such as title and security classification related to the record to provide contextual information on the record.

1. **Registration** formalizes the capture of records in the ERMS. A unique identifier for each record is generated as evidence that the record has been captured in the ERMS.
2. **Metadata**

The following are the standard metadata fields used in the records management environment.

a. Metadata about the record. This includes meta data about

i. reference code (unique identifier that links to the description)

ii. title (name of the record)

iii. name of creator

iv. date of creation

v. unit of description

vi. level of description (according to the File Classification Plan)

vii. other fields may be included as necessary

b. Metadata about policy, mandates and business rules.

c. Metadata about work processes.

d. Metadata about records management processes.

e. Others

Metadata need to be managed to ensure the authenticity, utility, integrity, and security of records over time for as long as the records are accessed. Metadata ensure that records cannot be altered without authorization. Only authorized persons shall have access to the metadata database. Any change shall be documented and should be auditable.

3. File Format.

File format affects accessibility of records. Changes in format may result in loss of access. This issue should be taken into consideration in the design of records preservation activities.

It is preferable to use non-proprietary formats especially those endorsed by international standards that are supported by more than one developer and can be read by many other software systems thereby allowing inter-agency and intra-agency sharing.

4. File Format Standard.

File formats can become obsolete rapidly due to continuous changes in technology. When converting from one file format to another, electronic records must remain authentic, unaltered, complete, accessible, and legally admissible in court throughout their approved retention periods. Records must be created in a trustworthy manner so that they may

meet legal and operational requirements.

Furthermore, standard formats for electronic records must be clearly identified to ensure accessibility and to facilitate future migration. Below is a table of file formats which may be updated regularly:

Type	**Primary Preservation Format (preferred)**	**Secondary Preservation Format (acceptable)**
Text/word processing applications	PDF	RTF (text) / TXT / XML with schema
Spreadsheet applications or structured data	PDF (must capture entire workbook - macros disabled)	CSV (Tab-delimited) TXT / XML
Presentations	PDF	Original (PPT)
Images	TIFF (uncompressed)	JPEG / PNG
Graphics	TIFF	PDF
Email	XML email preservation	
Database Management System	Keep in Original format	XML with schema
Websites and Social media records	WARC	ARC Files from content management system

Data migration. Data migration is the process of periodically converting electronic records to new file formats and/ or new storage media to ensure that records will remain usable for the entire duration of their authorized retention.

Data migration of electronic records shall be required when at least one of the following conditions is present:

1. The scheduled destruction date is greater than five years from the initial installation date or last major upgrade of the computer storage device or software that reads, process, or maintains the records.

2. The total retention period is greater than ten years from the date the records were created.

3. Usability will be affected by replacements, upgrades, or other changes in computer hardware or software components.

11.2 TRANSITIONING FROM PAPER RECORDS TO ELECTRONIC RECORDS:

As a prerequisite for implementation of ERMS, bank should develop a File Classification Plan and Records Disposition Schedule. The success of ERMS implementation depends on how well the strategies and plans are put into action. Hence, before transitioning from paper to electronic, the following steps must be undertaken:

1. Define the terms and objectives of the transitioning activity
2. Define the scope of the activity
3. Determine deliverables and target timeline / s
4. Identify project personnel
5. Establish and maintain communication channels
6. Ensure quality control
7. Prepare activity documentation
8. Establish evaluation procedures

11.3 ELECTRONIC RECORDS MANAGEMENT SYSTEM STANDARDS:

The ERMS must follow legal as well as administrative requirements and with national/international standards and best practices for electronic recordkeeping. The ERMS shall be guided by recorded/written policies and formal methodologies.

- **RECORD DOCUMENTATION.** Electronic records shall be created with essential metadata which describe the content and structure of the record as well as the background of its creation. Accurate and reliable links connecting the electronic record and the transaction that will be created shall be maintained.

  To ensure the accuracy of the information system's inputs and outputs, an ERMS shall include adequate controls, such as but not limited to the following:

  a. Audit trails

  b. Users' access level assignments

  c. Testing schedules

- **RECORD ACCESSIBILITY.** The content, structure, and context of records shall be transferred to and preserved in the ERMS in an accessible and useable format until the records reach the end of their retention period or until they are destroyed. Access to these records shall be allowed only after due authorization.
- **RECORD INTEGRITY.** All electronic records shall be properly secured. They shall be protected throughout their retention periods from intentional or accidental modifications, disclosures deletion, and unauthorized access. Permission to capture, access, or destroy electronic records shall only be given to authorized personnel.
- **RECORD SECURITY.** Bank shall formulate a set rule in line with industry standards on access levels to include the use of usernames and passwords. Access rights may be given to authorized users/personnel in accordance with risk profiling & applicable rules pertaining to confidential and classified records. The Bank shall also identify which electronic records are subject to legislative, regulatory, and institutional policy restrictions. One way of securing electronic records is encryption. This is the process of encoding electronic records so that only authorized users can open, decipher, and read them. Encryption can be applied while preparing for records transmission or while records are in storage.
- **OFFICIAL COPY.** An electronic record should be considered as the official copy when it is created, captured, and maintained within a reliable electronic recordkeeping system.
- **RECORDS INVENTORY.** Bank shall create a records inventory of all records, regardless of media. Electronic records identified shall be recorded and tagged with the following additional information:

  File size in bytes.

  Storage medium. File

  type.

  Status, whether original or reformatted.

- **RECORDS ELIGIBLE FOR CONVERSION.** Records with long-term administrative, legal, or other permanent value shall be prioritized for conversion to an electronic format.
- **WORK PROCESSES.** The creation and management of electronic records must be related with work processes, procedures, and tools. The work processes and electronic work environment shall be the bases of electronic recordkeeping, thereby guaranteeing that records are adequately captured, and are understandable/usable for immediate and long-term use.
- **DIGITAL SIGNATURE.** All accountable personnel of the bank who opt not to physically affix their signature to official documents must use official digital signatures. Digital signatures have verifiable metadata and are password protected. Scanned signatures are not acceptable as these are not digital signatures.
- **RETENTION AND DISPOSAL.** The retention and disposal of electronic records shall be in accordance with the approved records disposition schedules.
- **RECORD PRESERVATION.** It is to be ensured that electronic records should not be altered at all stages of their existence. Bank must ensure the future accessibility of electronic records by developing migration and conversion strategies that are designed to update hardware, software, and storage media before they reach obsolescence. The ERMS should be able to manage and preserve the content of the record as well as its metadata which define or document the record's context and structure.

11.4 STORAGE MEDIA.

The careful selection of the appropriate storage media is essential in designing an ERMS. Moreover, it should be noted that files may have to be refreshed or migrated to a different format at a selected time regardless of the storage media being used.

When selecting, it is important to note that electronic records storage may be done online or offline as well as near-line as guided by the following scheme:

1. Offline storage is for records which are not frequently accessed.

2. Online storage is for records which are used day to day. The

different kinds of storage are characterized as follows:

1. OFFLINE STORAGE. For stability, files that cannot be accessed instantly are to be stored offline such as records on removable media like external hard drives. The focus is on accuracy, protection, and security due to the need for long-term storage. The longer the retention period of the records, the more significant preservation methods, back-up procedures, storage conditions, handling procedures, and security become. Offline storage can be stored in-house, off-site, or outsourced.

Examples of offline storage include:

a. External hard drives (with moving parts)

b. Solid-state device

2. ONLINE STORAGE. Properly designed online storage permits prompt access to records to appropriate users only on the system's network. Online storage entails more expensive network storage but provides the maximum functionality.

3. FILE STORAGE WITH A THIRD PARTY. A third-party storage facility that can store, access, and deliver records can also be considered upon approval by the designated authority. Third-party services include management of offsite storage facilities as well as cloud computing technologies, both of which are contracted out. In selecting third-party storage, bank must assure that policies, procedures, and facilities of the service provider can meet the banks' operational needs, legal requirements, other existing laws on evidence and privacy. It is urged that records with security classification only be kept in in-house servers and not with third party servers.

4. CLOUD COMPUTING. To enable bank to share records and collaborate efficiently, the current trend is the establishment and operation of centralized data centers connected to a common network. Cloud computing service is the remote version of a data center where records are stored in a public cloud facility.

More than just file sharing, the cloud also allows users to access

documents if there is available internet connection. Cloud computing provides greater productivity because employees can access from any gadget and from any place. This is especially useful during emergencies and calamities. Joining the cloud provides users readily available backups for records and operations as well as business recovery after disasters.

Main considerations when deciding to join the cloud:

a. Preservation - There should be mechanisms in place to check the integrity of the records stored in the cloud. Cloud administrators must guarantee that long term or permanent records retain their original content, context, and structure while residing in the cloud.
b. Disposition - Data centers create multiple copies of records they store in different locations to ensure that data is not lost. Agencies should ensure that provisions are in place to allow the authorized destruction of all copies of records which have reached the end of their retention periods.

Selection of records for the cloud- Decisions on what records to upload must be carefully considered keeping in mind issues related to freedom of information and data privacy.

PART B – DATA RETENTION (HANDLING & RETENTION OF DIGITAL DATA)

12.1 Introduction:

Data retention is a part of an organization's overall Data Management framework, which needs to be retained for its business, legal, regulatory and compliance values. However, accumulating data and storing them indefinitely in the ecosystem can affect the performance of the IT Systems resulting in need for more computing powers and processing overheads. Similarly, retaining data longer than necessary, poses risks of data redundancy, data leakage, data breach etc, for which the Bank as Data Controller / Data Fiduciary, will be held accountable and may violate legal or regulatory requirements as forthcoming Data Protection and Data Privacy laws prescribe "Right to Forget" and "Right to Erasure". Therefore, it is necessary to create governance around Data Retention and disposal thereof to maintain optimum level of data to ensure performance efficiency and optimization of storage capacities.

- Data is a set of information, knowledge, facts, concepts, instructions or numbers, prepared or collected in a formalized manner or information in an electronic form that can be stored and used by a system.
- Digital Data is data that is created using IT or computer applications and can be interpreted by other applications.
- Data Retention is the process of continued storage of an organization's data for various compliance and business requirements for a specified period. It comprises of Active data and Archived data.
- Data Archival: Archived data consists of older data that remains in the storage system, which can be used as and when needed. Archival ensures that the Active Data storage stays lean.
- Data Purging or disposal is the method of erasure or deletion of data from the storage systems, which is no longer required. Purging deletes the data permanently and sets free the memory space or storage for other usage.
- Preservation means to keep the records in good order, preventing from being altered, damaged, or destroyed.

12.2 Roles & Responsibilities:

2.1 Information owner

This is a business executive or business manager who is responsible for a bank's business information asset. Responsibilities would include, but not be limited to:

- Assigning initial information classification and periodically reviewing the
- Classification to ensure it still meets business needs
- Ensuring security controls are in place commensurate with the classification
- Reviewing and ensuring currency of the access rights associated with information assets they own
- Determining security requirements, access criteria and backup requirements for the information assets they own
- Specify the retention period of Data for which no retention period has been prescribed in Bank's Policy on Record Retention.

2.2 Information or Data custodian

The information or Data custodian, usually an information system official, is the delegate of the information owner with primary responsibilities for dealing with backup and recovery of the business information. Responsibilities include, but are not limited to, the following:

- Performing backups according to the backup requirements established by the
- information owner
- When necessary, restoring lost or corrupted information from backup media to
- return the application to production status
- Ensuring record retention requirements are met based on the information owner's requirements

o Creation and maintenance of inventory of Data under custody.

o Data / Digital records are categorized according to the types of data mentioned in this Policy

o Mapping of data / digitized records with the physical equivalent records and assigning suitable retention period for each type of Data. Data Custodian shall specify the retention period of Data in consultation with the respective Data Owners, wherever retention period has not been assigned for the equivalent Records.

o Archival of the data as an intermediary stage, if required, keeping in view the operational requirements.

2.3 Application owner

The application owner is the manager of the business line who is fully accountable for the performance of the business function served by the application. Responsibilities, inter-alia, include:

- Establishing user access criteria, availability requirements and audit trails for their applications

- Ensuring security controls associated with the application are commensurate with support for the highest level of information classification used by the application

- Performing or delegating the following - day-to-day security administration, approval of exception access requests, appropriate actions on security violations when notified by the security administration, the review and approval of all changes to the application prior to being placed in the production environment, and verification of the currency of user access rights to the application.

12.3 Internal Audit / Inspection

Implementation of Data Archival / Disposal / Purging shall be verified during the Internal Audit / IS Audit of the concerned Application Owners.

a) The preservation of documents should be such as to ensure that there is no tampering, alteration, destruction or anything which endangers the content, authenticity, utility or accessibility of the Documents.

b) The preserved documents must be accessible at all reasonable times. Access may be controlled by Authorized Officer, so as to ensure integrity of the documents and to prohibit unauthorized access.

12.4 Types Of Digital Data/ Digitized Records

Data in Bank's ecosystems are broadly classified as under:

i. Application Data

ii. Logs / Audit Trails

iii. Business-related Customer & Transaction Data

iv. Voice Recording / CCTV Footage

v. Electronic Mail (E-mail)

vi. Biometric Data

vii. Digitised Records

viii. Reports / Dashboards / MIS etc.

ix. Miscellaneous Data not covered in above categories

i. **Application Data:** It includes Application Binaries, Operating System, Virtual Machines, Database and related data that constitutes the application supporting a functionality or the Business Process. It also includes configuration files related to the components of the Application set-up, Parameter files etc.

ii. **Logs / Audit Trails:** It consists of chronological record of events like user login, file access, other various activities to indicate what action was attempted, who performed the action, when it was performed and if it was successful or unsuccessful. It also includes activities such as updates and patching to determine when a system component fails or incorrectly configured e.g. Logs related to Operating System, Database, Applications, Middleware, Virtual Machine, Server, Network Devices Tools etc.

iii. **Business-related Customer & Transaction Data:**

This includes Business Data & Insights related to Customer and Transaction such as:

a) Digital and digitized Data or insights pertaining to customer like personal details (Name, DOB, address, Mobile Number, Email IDs, any PII data, etc.)

b) Data related to Customer's Account (Product, Term, Rate of Interest, etc.)

c) Financial or non-financial or both data/details of transactions such as debits / credits in those accounts.

iv. **Voice Recording:** Voice recording through devices with recording features over the phone, device (e.g. Customer Contact Center, Dealing Room Operations etc.) or via an online-meeting application (e.g. MS Teams/Webex etc.).

v. **CCTV Footage:** Closed-Circuit Television (CCTV) is a system that records video/audio footage installed in the Branches, Offices, Establishments, ATMs, Data Centers etc. as part of security, surveillance and monitoring of access controls etc. Video Footage is also referred to by various internal and external agencies such as regulator, security agencies, auditors etc.

vi. **Electronic Mail (E-mail):** In today's time E-mail is the fastest and most convenient mode of transmission for messages or information and effectively it is the same thing as sending a memo or a letter in "hard copy". As such, electronic mail can be an official record of the Bank. Electronic mail systems are not designed as recordkeeping systems. This means that management of electronic mail is not part of the system design, rather e- mail needs to be managed by understanding what types of records are created using e-mail communication systems.

vii. **Biometric Data:** Fingerprints or any other similar bio-identifiers, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifiers used to identify an individual. It is the personal information stored by Bank about an individual's (e.g. employees, customers, vendor resource etc.) physical characteristics that can be used to identify that person. The purpose of collecting or obtaining such biometric data and usage shall be defined by the respective Data Owner, who shall specify the period of retention and purging or deletion frequency in the event of ceasing of relationship with the individual concerned like retirement/termination/transfer of employee, end of relationship with the customer, end of contract with the vendor etc.

viii. **Digitised Record:** is the digital representation of record, converted from physical or analogue records through scanning or imaging such records.

ix. **Reports / Dashboards / MIS:** IT Departments prepare reports (Regulatory, MIS), dashboards etc. keeping in view various business requirements in consultation with the respective Report Owners (The Business Units on whose behalf such Reports / Dashboards have been prepared)

x. **Miscellaneous Data:** Data which is not mapped with any specific data type as mentioned above or any new data category which may come up in the future.

12.5 Disposal/ Purging of Digital Data/Records:

Storage of business-sensitive data is critical but ever-increasing volume of digital data, which is further set to expand manifold, requires scientific management. Carrying bulky database, without their archival / disposal / purging since Bank's migration to CBS, has resulted in multiple challenges including possible data breach and regulatory non-compliance.

Disposal of data, beyond their reasonable retention period, shall have following benefits:

a) Process improvement & Increased Efficiency:

i. Maintaining data quality throughout its lifecycle.

ii. Ensuring availability of accurate and reliable data to users for various business requirements.

iii. Managing challenges of exponential and/or uncontrolled growth in database due to massive digital transactions such as UPI.

iv. Improving System performance and efficiency due to lower requirement of computing power.

v. Simplifying the present complex of digital ecosystems.

b) Reduced cost of storage (On-Premises or even on Cloud):

i. Reducing costly maintenance of abnormally large database

c) Compliance and Governance:

i. Maintaining compliance with data privacy laws and compliance with evolving regulatory / statutory requirements.

ii. Ensuring retention of right set of data along with right amount of data for right duration.

iii. Mitigating Operational Risk, including possibility of data breach.

After expiry of the retention/archival period, the Department Head shall recommend and obtain approval for purging/disposal of the Data.

Respective Data Custodian / Department shall purge / dispose the digital as well as their digitized versions from all locations whether in database records, cloud storage, backup files etc. or in physical storage media such as CD-ROMs, DVDs, backup tapes, hard drives, mobile devices, portable drives.

Destructions of physical media, computers, servers etc., if any, shall be handled as per the guidelines contained in the latest IS Policy & IT Asset Disposal Policy.

List of Records containing the details of purging / disposal, of data shall be preserved permanently, along with evidence of having purged/disposed a particular data, which might be required to be produced to any Court, Statutory Body, Regulator, Auditor etc. in support or as evidence of having purged/disposed the Data.

Periodicity of Archival /Disposal/Purging: Data Archival will continue as per the appropriateness decided by the respective Application Owners. 1st June of every year shall be the cut-off date for Data Disposal / Purging. Archival and disposal periodicity of Customer and Transaction related data.

12.6 Data Archival

Data Archival may involve processes that may require transferring data from storage to Secondary storage or an alternate central storage server or system for long term retention.

Define a mechanism to move data from retained status to purging /disposal. Data in these stages to be identified and segregated without any overlap. A Centralized Log Archival Solution may be explored supporting & managing an organization's entire data lifecycle.

Put in place an automated system for identifying the data/records for purging/disposal and carrying out the exercise of purging/disposal at a pre-defined periodicity. Periodic review (recommended at least annually) for retention / deletion / purging of data.

List of Critical and Non-Critical applications defined in BCP and DR Policy

IT Assets	Critical Applications	Risk - Profiling	Non-Critical Applications	Risk - Profiling
Software programmes (From Software Version expiry date)	10 Years	High	5 Years	Medium
OS & Applications system software				
Device configurations				
Source codes after withdrawal of package from production environment.				
Data archives (on media)				

(a) The applications not mentioned in either Critical or Non-Critical category as per BCP Policy, will have retention period of 5 years unless otherwise specified by the respective user departments.

(b) Retention, Archival and Disposal of Digital Data/ Record pertaining to Customers i.e CIFs, Accounts and Transaction Data – Trigger: After Closure of Accounts or Relationship -10 years

(c) The period mentioned is the overall timeframe for retention of data by the bank irrespective of whether the same is maintained in the source/archival system.

(d) The classification and preservation period for the digital records will be done in line with Chapter 7.4 of the policy i.e. Classification of Record Preservation. The Risk Profiling for digital records is done in line with chapter 7.5 of the policy

Retention of Email:

The retention period of emails for a period of 10 Years from the date of email (regardless of deletion by end user).

IT Related Data: The records pertaining to IT Department whether held in physical/digital format, retention period is mentioned in Annexure -1

Periodicity of Archival /Disposal/Purging:

Data Archival will continue as per the appropriateness decided by the respective Application Owners. 1st June of every year shall be the cut-off date for Data Disposal / Purging. The period of archival being an internal decision/preference the same shall be mutually agreed upon by the data owners & data custodians.

Annexure -1

Sl. No.	Records to be preserved managed by IT department	Period of Retention	Risk Profiling
1	Bills Payment Register	5 Years	Medium
2	ITD related Sanction Note files	5 Years	Medium
3	Sanction given to RO/RCC by ITD	5 Years	Medium
4	AMC & ATS files and related documents, post Contract Expiry	5 Years	Medium
5	Tender opening register	5 Years	Medium
6	Software Development life cycle documents and change management document	5 Years	Medium
7	Purchase Order Register/file post Contract Expiry	5 Years	Medium
8	Service Level Agreements and Non Disclosure Agreements, post Contract Expiry	5 Years	Medium
9	All RFP / Tender documents from contract expiry date	5 Years	Medium
10	IT related Audit Reports (Internal & External)	5 Years	Medium
11	Reply to Audit Reports (IS Audit / IS Security / other Audit – Reply to CSITE, etc.)	5 Years	Medium
12	IOBONLINE-archives	5 Years	Medium

13	Standard Operating Procedures	10 Years	Medium
14	Project Files of completed projects	10 Years	Medium
15	Customer related data on media	10 Years	Medium

12.7 Regulatory Directions on Audit Logs Retention

Regulatory Directions on Audit Logs Retention

- Audit logs shall be preserved for a period of at least five years. [CERT-In Directions 70B dated: 28.04.2022]
- The logs that should be maintained for a period of at least five years such as Firewall logs, Intrusion Prevention Systems logs, SIEM logs, PAM logs (Video/text), Classification logs, web / database/ mail / FTP / Proxy server logs, Event logs of critical systems, Application logs, ATM switch logs, SSH logs, VPN logs etc. It may be noted that this list of logs is not exhaustive but has been mentioned to provide flavour of logs to be maintained by the relevant teams. From the incident response and analysis perspective both successful as well as unsuccessful events shall be recorded.
- Stockbrokers / Depository Participants should ensure that records of user access to critical systems, wherever possible, are uniquely identified and logged for audit and review purposes. Such logs should be maintained and stored in a secure location for a time period not less than two (2) years. [SEBI Cyber Security & Cyber Resilience framework for Stockbrokers / Depository Participants (03rd Dec-2018)]
- Data Centres, Virtual Private Server (VPS) providers, Cloud Service providers and Virtual Private Network Service (VPN Service) providers, shall be required to register the following accurate information which must be maintained by them for a period of 5 years or longer duration as mandated by the law after any cancellation or withdrawal of the registration.

Sl.No.	Records to be preserved	Period of Preservation	Risk Profiling
1	Syslog (SIEM Log)	5 Year	Medium
2	PAM Logs (Video/Text)	5 Years	Medium
3	Classification Logs	5 Years	Medium

12.8 Exception handling:

Where any decision or proposition with respect to digital/digitized data maintenance, results in retention schedules not being in conformity with the schedule defined in this Policy, the same shall be approved by the concerned Vertical Head not below the rank of General Manager.

- The Data Custodian / Department shall record the justification to modify any data category or retention schedule and document and maintain the same along with the required approval and advised to respective Data Owner.
- Change in category of a Data, thereby resulting in a change in the retention schedule shall also require approval.

PART C – PRESERVATION PERIOD OF RECORDS - FOR DEPARTMENTS AT CENTRAL OFFICE

Banking Operations Department &

Inter Branch Reconciliation:

Sl.No.	Records to be preserved	Period of Preservation	Risk Profiling
1	Branch Visit Reports	1 Year	M
2	Charges statement of Regional Offices	2 Years	M
3	Suspense and Sundry Creditors Review	2 Years	M
4	IBIT/FT Statement file	3 Years	M
5	CAS closed correspondence file	3 Years	M
6	CO/DDR Summaries and enclosures	5 Years	M
7	All Registers	5 Years	M
8	Vouching Check List/Fair List/Adjustment books	8 Years	M
9	Loss of Drafts / Deposit Receipts – Circulars	8 Years	M
10	Approved List of Lorry Companies	8 Years	M
11	Board Notes/ TMC-files	Permanently	M
12	Selective credit control directives	Permanently	M
13	ECGC Circulars	Permanently	M
14	Interest Rate (Advances) Circulars Discretionary powers/ Service charges/ Locker Rent –circulars Share Clearance Register / file	Permanently	M
15	CO/DDR Remittance summaries	Permanently	M
16	Books relating to merged / segregated entries	Permanently	M

Planning Department:

Sl.No.	Records to be preserved	Period of Preservation	Risk Profiling
1	Conference material	2 Years	M
2	Correspondence with Regional Offices file	2 Years	M
3	Periodical review of Regions performance	2 Years	M
4	Quarterly Branch visits by Regional Managers – Reports.	2 Years	M
5	Industry wise and sectoral Flow of credit	5 Years	M
6	Export credit data	5 Years	M
7	Office Note	5 Years	M
8	TMC Notes	25 Years	M
9	RBI-correspondence file	25 Years	H
10	Board Notes relating to Performance Budgeting , Credit Planning, Branch Expansion, Costing and MOU cell	Permanently	H
11	Licenses of Branches/ Extension Counters	Permanently	H
12	License Register	Permanently	H
13	Studies conducted by Costing Cell and other Sections of the Department	Permanently	H

General Administration Department:

Sl.No.	Records to be preserved	Period of Preservation	Risk Profiling	Remarks
1	Letters Received Register	2 Years	M	
2	Dispatch Register	2 Years	M	
3	Files related to lease of vacated premises	5 Years	M	
4	Application / Sanctions related to Lease of Officers Quarters	5 Years	M	Maintained electronically
5	Mobile Handset Expenses reimbursement	5 Years	M	Maintained electronically

6	Empanelment files from the date of empanelment	5 Years	M	
7	NIT / RFP / Tender Documents/particulars.	5 Years	M	
8	AMC Contract files from the date of award of work	5 Years	M	
9	Files related to Purchase of cars & accessories etc.	8 Years	H	
10	Petty Cash Register	10 Years	M	
11	Registers –Suspense/Sundry creditors/Banker's cheques/ Capital work-in-progress	10 Years	H	
12	Rent Paid details pertaining to officers leased quarters	10 Years	H	
13	Major repair and renovation project files.	10 Years	H	
14	Tender Opening Register	10 Years	H	
15	Records pertaining to capital expenditure	15 Years	H	
16	Records pertaining to residential furniture's/mattresses sanctioned to officers	15 Years	H	Maintained electronically
17	Records related to Furnitures; Fixtures & other office equipment's purchased for offices & Banks' owned quarters	15 Years	H	
18	Banks' Owned Quarters Allotment Register	Permanently	H	
19	Files related to lease agreements of Branches/Regional Offices / other offices	Permanently	H	
20	All Bank owned property documents	Permanently	H	
21	Recorded memorandums and ATRs - Board / Management Committee of Board / TMC / AC-ED / AC-GM (CO)	Permanently	H	
22	All Capital Projects including purchase of property, new construction etc.	Permanently	H	

LEAD BANK:

Sl.No.	Records to be preserved	Period of Preservation	Risk Profiling
1	Returns received from Regional Offices, Member Banks and Lead District managers	5 YEARS	M
2	Agenda and Minutes received from all the districts of Tamil Nadu	5 YEARS	M
3	Letters received/ Despatch register	5 YEARS	M
4	General correspondence file after the closure related matters	3 YEARS	M
5	Reference file	5 YEARS	M
6	Data Bank file	5 YEARS	M
7	Office Copies of returns submitted to RBI/ NABARD	10 YEARS	H
8	Annual Credit Plan booklets for each District	10 YEARS	H
9	Attendance Register	10 YEARS	H
10	Board Notes file	Permanently	H
11	RBI and NABARD circulars	Permanently	H
12	Guidelines on various Government sponsored Schemes	Permanently	H
11	Library Register	Permanently	H
12	SLBC Agendas and minutes	Permanently	H

MSME Department:

Sl.No.	Records to be preserved	Period of Preservation	Risk Profiling
1	All MOUs, after expiry	5 YEARS	M
2	All MIS Reports	10 YEARS	M
3	TUF Files, after closure of Accounts	10 YEARS	M
4	SME – RBI Circulars	Permanently	M
5	Guidelines on various schemes	Permanently	H
6	CGTSSI / CGTMSE / CGFMU Circulars	Permanently	H
7	Board Notes, Green Files	Permanently	H
8	CAF-1A review notes	Permanently	H
9	All borrower files	Permanently	H

Board Services Department:

Sl. No.	Records to be preserved	Period of Preservation	Risk Profiling	Remarks
1	All Files and Records	Permanently	H	Physical / Electronic

Credit Support Services Department

Sl. No.	Records to be preserved	Period of Preservation	Risk Profiling
1	Minutes of Meetings, Notes and Disposals of HLCC (GM) & HLCC (ED)	10 Years	H
2	Minutes of Meetings, Notes and Disposals of NBC & IT Screening Committee	10 Years	H
3	Reimbursement claims submitted to NABARD / STATE GOVT. / CENTRAL GOVT/DGFT/RBI (Export Interest subvention are reimbursed from DGFT/RBI)	10 Years	H

Public Relations Department:

1	Files-donations: Visit of parliament Committees	5 YEARS	M
2	Files related to Important functions celebrated by our Bank	5 YEARS	M
3	Profit and Loss registers and files relating to advertisement / sponsorship under Publicity Budget	8 YEARS	H
4	Board Notes file	Permanently	H
5	RBI and Ministry of Finance directives –files	Permanently	H

LAW DEPARTMENT & SAMD:

Sl. No.	Records to be preserved	Period of Preservation	Risk Profiling	Remarks
1	Inward letters Register	5 YEARS	M	Hard copy of the record is to be maintained for future reference.
2	Despatch Register	5 YEARS	M	Hard copy of the record is to be maintained for future reference.
3	Claim against Bank case files after final disposal and statements received from ROS	5 YEARS	M	Files in physical form are to be maintained for reference.
4	Reference on miscellaneous legal matters (after disposal of the related issues referred)	5 YEARS	M	Hard copy is maintained by the department for further reference if any.
5	Legal Opinions of general nature	5 YEARS	M	Hard copy is maintained by the department for future reference if any.
6	Claim Papers of accounts of deceased customers	8 YEARS	H	Hard copy of the record is to be maintained to defend future litigations.
7	Reply to RTI Queries	5 YEARS	H	Hard copy is maintained by the department for further reference if any.

8	Records relating to Deletion of Advocates	5 YEARS	M	Lawyers are challenging their deletion in Court. Hence, the papers need to be preserved at least for 5 years
9	Circulars issued by the Department	Permanently	H	
10	Register of Panel Lawyers	Permanently	H	The Register of Panel Lawyers is maintained in online in digital form.
11	Empanelment files from the date of empanelment	Permanently	H	The period of preservation should be made 'Permanent' as the records are required till the advocate is deleted from the panel.

RISK MANAGEMENT DEPT:

Sl. No.	Records to be preserved	Period of Preservation	Risk Profiling
1	Various Study notes placed to top management on Concentration Risk, Stressed sectors, Liquidity Ratio, Stock approach, Reputation Risk and Downtime analysis etc.,	3 Years	M
2	Correspondence with Regional Offices/departments	5 Years	M
3	Copies of Quarterly CRCC reports submitted by Regional Offices/Overseas branches/branches.	5 Years	M
4	CRCC un-availed/un-hedged declarations submitted by the branches.	5 Years	M
5	STL/LR/IRS/LCR reports submitted to RBI	5 Years	M
6	Daily LR/STL reports	5 Years	M
7	MID office reports.	5 Years	M

8	Copies of Preventive Vigilance meetings & OR statements submitted by Regional Offices/Zonal Offices	5 Years	M
9	Miscellaneous files related to staff matters.	5 Years	M
10	Approved Notes of RMA Rating validation	5 Years	M
11	Financial Disclosures data/outsourcing reports submitted to RBI/BSMD etc.,	5 Years	M
12	Agendas, minutes, action and ATR of all Risk Management Committee meetings i.e ORMC, CPC, ALCO and PRMC.	5 Years	M
13	RMCB, ACB, MCB and Board approved Notes relating to Policies, Studies, information notes etc.,	Permanently	H
14	Agenda files submitted to GM, EDs & MD & CEO for various meetings of Risk Management Department.	Permanently	H
15	Agenda Files submitted to GM, EDs & MD & CEO for RMCB & Board.	Permanently	H
16	ALCO/CPC/ORMC/PRMC background papers.	Permanently	H
17	Copies of RBI/Basel guidelines, study materials/magazines etc.,	Permanently	H
18	Reply submitted to RBS/RBI/AFI.	Permanently	H

CREDIT MONITORING DEPT:

Sl.No.	Records to be preserved	Period of Preservation	Risk Profiling
1	All review notes put up to ACB / Management Committee of Board / Board / GM Committees	Permanently	M
2	All Staff accountability files	Permanently	M

3	CSS review notes	Permanently	M
4	Quarterly Review Note on slippages during the quarter put up to ED / CMD / MD&CEO.	Permanently	M
5	SMA Review notes.	Permanently	H
6	Stock Audit Review Reports	Permanently	H
7	LRM Review Reports	Permanently	H

VIGILANCE DEPT:

Sl.No.	Records to be preserved	Period of Preservation	Risk Profiling
1	Files relating to Vigilance and non- vigilance cases relating to employees	Permanently	H
2	Monthly report of the Regional Vigilance Officers (RVOs)	Permanently	H
3	Dispatch registers	Permanently	H
4	Complaints	Permanently	H
5	Statements/ Returns	Permanently	H
6	Documents related to clearances	Permanently	H

FRAUD AND RISK MANAGEMENT CELL:

Sl.No.	Records to be preserved	Period of Preservation	Risk Profiling	Remarks (PERIODICITY)
1	Fraud reported files consisting of office notes, minutes, and other enclosures	Permanently	H	As & when
2	Quarterly Audit certificate	Permanently	H	Quarterly
3	Suspense debit permission approval notes	5 Years	M	As & when
4	Police & CBI complaint on frauds to be preserved by Branches/ ROs	Permanently	H	As & when
5	Committee for Monitoring Large Value frauds (CMLVF) agenda, minutes	Permanently	H	As & when And quarterly

6	ORMC-Fraud reported during the month, ACE-Review of Staff committed frauds during the month: agenda, minutes	Permanently	H	Monthly
7	ACB- Quarterly Review of frauds, CRDC agenda, minutes	Permanently	H	Quarterly
8	Board-Annual Review of frauds agenda, minutes	Permanently	H	Annually
9	Policy on Fraud Risk Management & Fraud investigation functions	Permanently	H	Annually
10	EFRM RFP, PO, SOP, Regulatory documents, Fraud Reported and other Documents	Permanently	M	As & when

TREASURY (DOMESTIC) DEPARTMENT:

Sl.No.	Records to be preserved	Period of Preservation	Risk Profiling
1	IBR statements received from Regional Offices	10 Years	M
2	Statements of RBI Account.	10 Years	M
3	All used files from the date from closure	10 Years	M
4	Interest advice files	10 Years	M
5	Correspondence – FEDAI/RBI/Branches	5 Years	M
6	Special Fortnightly returns	10 Years	M
7	Interest provision on Call Money transactions	10 Years	M
8	Paid COD receipts / related files.	10 Years	M
9	Contract Note File	10 Years	M
10	F.75 consolidation	10 Years	M
11	Form A and Form X Registers/returns	10 Years	M
12	All books / registers / Ledgers/ Balance books	10 Years	M
13	Funds Books	10 Years	M

14	Government Securities Registers or Ledgers	10 Years	M
15	Registers or ledgers of Bank's own investments	10 Years	M
16	Deals slips/position sheets/ R returns.	10 Years	M
17	Matters relating disputes/cases/Vigilance matters	Permanently	H
18	Agency Arrangements with foreign correspondence including private exchange houses	Permanently	H
19	Office notes relating to policy decisions and guidelines, procedures/ background papers in respect of permanent circulars	Permanently	H
20	Copies of all recorded Board Note	Permanently	H
21	IR/CAR reports.	Records to be preserved till Next Inspection by RBI/AFI/STATUTORY AUDITORS /INSPECTION DEPARTMENT	M

TREASURY (FOREIGN) DEPARTMENT:

Sl.No.	Records to be preserved	Period of Preservation	Risk Profiling
1	All used files from the date from closure	7 Years	M
2	Correspondence – FEDAI/RBI/Branches	5 Years	M
3	Matters relating disputes/cases/Vigilance matters	Permanently	H
4	Agency Arrangements with foreign correspondence including private exchange houses	Permanently	H

5	Office notes relating to policy decisions and guidelines, procedures/ background papers in respect of permanent circulars	Permanently	H
6	Copies of all recorded Board Note	Permanently	H
7	Deals slips/position sheets/ R returns.	Records to be preserved till Next Inspection by RBI/AFI/STATUTORY AUDITORS /INSPECTION DEPARTMENT	M
8	IR/CAR reports.	Records to be preserved till Next Inspection by RBI/AFI/STATUTORY AUDITORS /INSPECTION DEPARTMENT	M

CENTRALIZED FOREX PROCESSING:

Sl.No.	Records to be preserved	Period of Preservation	Risk Profiling	Remarks
1	Export Realization Bills (LC/Non- LC)	10 Years	H	Electronically
2	Outward remittance documents	10 Years	H	Electronically
3	Guarantee Document (Foreign)	10 Years	H	Electronically
4	LC opening Application	10 Years	H	Electronically
5	Import Bills (LC/Non-LC)	10 Years	H	Electronically
6	Inward Remittance documents	10 Years	H	Electronically
7	Trade Credit Documents	10 Years	H	Electronically
8	RBI referred documents	10 Years	H	Electronically

CORPORATE CREDIT DEPARTMENT:

Sl.No.	Records to be preserved	Period of Preservation	Risk Profiling
1	Other miscellaneous including inters department correspondence/statistics/MIS reports	2 Years	M
2	Files of closed Loan accounts [normal closure]	5 Years from closure	M
3	All back papers [like RO/Branch recommendation, balance sheet CMA query and query reply annexure to the RO/Branch recommendations]-regular running file	8 Years	M
4	ALL credit notes & sanction endorsements [both proposals & miscellaneous request]-Green File	10 Years	H
5	Files under investigation from various authorities [live or closed accounts]	Permanently	H

SECURITY DEPARTMENT:

Sl.No.	Records to be preserved	Period of Preservation	Risk Profiling
Files:			
1	Correspondence with CO Depts	5 Years	M
2	General Correspondence with Regions (Region Based)	5 Years	M
3	Crime reported by Regions (both Actual & Attempted)	5 Years	M
4	RSO Branch / CC Visit reports	5 Years	M
5	Guards & Guns Correspondence with Regions	5 Years	M
6	CSO Correspondence	5 Years	M
7	CSO Visit reports	5 Years	M
8	Staff Supervisory Correspondence	5 Years	M
9	Sub-Staff Correspondence	5 Years	M
10	Sub-Staff Allowances	5 Years	H
11	Fire & Security Gadgets - Central Office	5 Years	M
12	Budget	5 Years	M
13	Uniform & Liveries - Guards CO	5 Years	M
14	Cash Van Correspondence / Returns	5 Years	M
15	Court Cases	Till disposal	M
16	Training	5 Years	M
17	Administration	5 Years	M
Registers:			
1	Attendance Register	5 Years	M
2	Visitors Register	5 Years	M
3	Workers Register	5 Years	M
4	Courier Register	5 Years	M
5	Vehicle Register	5 Years	M
6	Fire Incidents	Permanently	M

7	Duty Register for guards	5 Years	M
8	Fire Drill at Central Office	5 Years	M
9	Mail in Register	5 Years	M
10	Dispatch Register CO	5 Years	M
11	Dispatch Register Regions	5 Years	M

BALANCE SHEET MANAGEMENT DEPT:

Sl.No.	Records to be preserved	Period of Preservation	Risk Profiling
1	Daily voucher pad	Permanently	M
2	General Ledger/GL monthly extract	Permanently	M
3	Day book	Permanently	M
4	Profit and Loss supplementary /Ledger	Permanently	M
5	Bank Balances ledgers (Nostro accounts)	Permanently	M
6	Bank supplementary / Ledger	Permanently	M
7	Unclaimed Balances Accounts Ledgers and statements received from Branches	Permanently	M
8	Suspense/ Sundry Creditors ledgers	Permanently	M
9	Tax Audit Report	Permanently	M
10	Return of Income	Permanently	M
11	Assessment Orders	Permanently	M
12	Appeal papers	Permanently	M
13	Appellate Orders	Permanently	M
14	Other correspondences related to Income Tax	Permanently	M
15	All DSB returns submitted to RBI	Permanently	M

Investor Relations Cell:

Sl.No.	Records to be preserved	Period of Preservation	Risk Profiling
1	Minutes of EGM / AGM	Permanently	M
2	Share transfer memorandum books / Board notes / Minutes	Permanently	M
3	Share grievance Committee Board note / Minutes	Permanently	M
4	All the files relating to lower tier II and upper tier II	Permanently	M
5	All files relating to perpetual tier I instruments	Permanently	M
6	Dividend payment files	Permanently	M
7	Annual Reports	Permanently	M
8	AGM / EGM related files	Permanently	M
9	Files relating to raising of Capital	Permanently	M
10	Constitution of share transfer, share grievances and director appointment files.	Permanently	M
11	Share holding Pattern	Permanently	M
12	Corporate Governance files	Permanently	M
13	NSE and BSE files	Permanently	M
14	SEBI related matter files	Permanently	M
15	Files related to quarterly compliance	Permanently	M
16	Quarterly results submitted to NSE and BSE in the SEBI format file	Permanently	M
17	Policy on appointment of Statutory Central Auditors and Statutory Branch Auditors	Permanently	M

OFFICIAL LANGUAGE DEPARTMENT:

Sl.No.	Records to be preserved	Period of Preservation	Risk Profiling
1	Original Training / Intensive Training Schedule File	5 Years	M
2	CO Circular, translation matter and Printing and stationery matter	5 Years	M
3	Inspection report on Branches by Inspection Department ,CO	5 Years	M
4	Dispatch Register and Translation entry/exit register	5 Years	M
5	TOLIC –Competition Winners File	3 Years	M
6	Competition Result File (Hindi Day, All india Hindi Essay, Reserve Bank (in-house) House magazine , Raj Bhasha (in-house), Hindi Day Competitions –Winners List	5 Years	M
7	Evaluated Examination Answer Papers IOB Praveen Course	10 Years	M
8	QPRs, OLIC Minutes and Half-yearly Reports received from Regional Offices	5 Years	M
9	Leave Records, Copies of Documents and Papers pertaining to Staff members who have left Bank's service on superannuation/VRS	5 Years	M
10	Copies of QPRs sent to Ministry/RIO, Department of Financial Services	5 Years	M
11	Hindi classes Application of Members and Hindi Class Attendance Register, Honorarium Payment Register	10 Years	M
12	Exam fee, Exam Day Conveyance, and related matters.	5 Years	M

13	Attendance registers, Leave registers, OLIC Register	5 Years	M
14	Central Office-Official Language Department circulars, Official Language Manuals	5 Years	M
15	Central office-Official Language Implementation Committee Minutes Register	Permanently	M
16	Annual Action plan of Ministry of Home Affairs, Government of India	10 Years	M
17	Office Memorandum, Directives, Instructions, Guidelines of Ministry of Home Affairs, Ministry of Finance (Banking Division), Government of India	10 Years	M
18	Inspection of central offices, Branches, by Ministry of Home Affairs, Ministry of finance (Banking division), Government of India	10 Years	M
19	Parliamentary Committee on official Languages –Visits , reports , replies (Central Office, regional Office, Branches)	Permanently	M
20	Inspection file of Area Implementation Office, Kochi-of Ministry of Home Affairs	10 Years	M
21	Ministry of Home Affairs – Prabodh, Praveen, Pragya , Hindi typing, Hindi Stenography Exam Results , BOH Exam Results/Unicode Training list.	10 Years	M
22	Cash Incentive Sanction Register	Permanently	M
23	Half-Yearly report on Official Language Implementation submitted to Board	5 Years	M

24	IOB Praveen file (containing particulars on question paper setting, evaluators , examination day expenditures , central office exam arrangement expenditures)	10 Years	M
25	Shields, Certificates, Cups and photographs of important Events	3 Years	M
26	Office Notes, files, roster (with regular changes and updation).	5 Years	M
27	Back –up CDs	Permanently	M
28	Sponsoring Official Language Activities , Donations etc., File	10 Years	M
29	Vani Printing File (Quotation, Expenditure) etc.	5 Years	M
30	Hindi Day Celebrations : Statement of accounts and expenditure	5 Years	M
31	Routine letters and correspondence , Bilingual format file	5 Years	M
32	Official Language Systems, Procedure, rationalization File	5 Years	M
33	Hindi Library Books, Library Purchase and stock Registers and Movement Register, specimen of Hindi /BL/TL Documents ,Registers , Brochures, Pamphlets, Publications	Permanently	M
34	Half-Yearly report submitted to TOLIC	3 Years	M
35	Various Report submitted to Compliance Department	5 Years	M
36	Quarterly report submitted to Investor Relation Cell	5 Years	M
37	All ROs file	5 Years	M
38	Staff Matter	5 Years	M

KYC – AML DEPT:

Sl.No.	Audit Reports to be preserved	Period of Preservation	Risk Profiling	Frequency of report	Remarks
1	RBI Audit report	5 Years	M	Yearly	Physical/Electronic
2	IS Audit report	5 Years	M	Yearly	Physical/Electronic
3	Management audit report	5 Years	M	Yearly	Physical/Electronic
4	Vendor Audit	5 Years	M	Yearly	Physical/Electronic
5	FIU Review	5 Years	M	Yearly	Physical/Electronic
6	Statutory Audit	5 Years	M	Yearly	Physical/Electronic
7	IFCOFR	5 Years	M	Yearly	Physical/Electronic
8	ACE and ACB meeting Minutes	5 Years	M	As and when conducted	Physical/Electronic
Sl.No.	**Regulatory Reports to be preserved**	**Period of Preservation**	**Risk Profiling**	**Frequency of report**	**Remarks**
1	STR, NTR, CBWTR,CCR, CTR	5 Years	M	Monthly	Physical/Electronic
2	ML/TF Risk assessment of the bank	5 Years	M	Yearly	Physical/Electronic
3	Screening reports	5 Years	M	As & when updated	Physical/Electronic
4	Law Enforcement agencies correspondence	5 Years	M	As & when received	Physical/Electronic
Sl.No.	**Miscellaneous Reports to be preserved**	**Period of Preservation**	**Risk Profiling**	**Frequency of report**	**Remarks**
1	Mail correspondence	5 Years	M	Daily mails to branches, departments, and LEAs	Physical/Electronic
2	Notes to Other departments	5 Years	M	As and when initiated	Physical/Electronic
3	AMLOCK reports	5 Years	M	Need based	Physical/Electronic
4	Vendor agreements	5 Years	M	From ending business relationship	Physical/Electronic

Records to be preserved for indefinite period:

A) If the matter related to a suspicious transaction is pending in a court, the relevant records to be retained for 5 years from the date of final verdict of the court.

B) In cases, where RBI /FIU-IND or any other regulatory body requests for the retention of records for a period more than 5 years , bank should be guided by such specific requests.

INSPECTION DEPT:

A. Records to be preserved for FIVE years

Sl.No.	Audit Reports to be preserved	To be preserved by whom	Risk Profiling	Frequency of report	Remarks
1	Concurrent Audit reports of branches	Branch/RO /Inspectorate	M	Monthly	Hard copy at branch Soft copy at RO/ Inspectorate
2	Revenue Audit reports of branches	Branch/RO /Inspectorate	M	Yearly	Hard copy at branch and soft copy at RO (if soft copy is not received, Hard copy to be preserved
3	Concurrent Audit reports of CO Departments	Central Office, Inspection Dept.	M	Monthly	Hard Copy
4	IS Audit Reports of RCCs	IS Audit Cell, CO, RCC at RO	M	Yearly	Hard Copy
5	DC Audit, DR Audit of DR Centers, SWIFT & NLS	IS Audit Cell, CO & at ITD, CO	M	Quarterly	Hard Copy
6	RACE Minutes	RO, Inspection Dept.	M	Monthly	Hard Copy
7	ACE meeting Minutes	Inspection Dept, CO	M	As and when conducted	Hard Copy
8	IS Audit reports of CO Departments	IS Audit Cell, CO & at ITD, CO	M	Annually	Hard Copy
9	IS Audit reports of Branches wherever it is conducted	IS Audit Cell, CO & at ITD, CO	M	Yearly	Hard Copy
10	Concurrent Audit report of Finacle	IS Audit Cell, CO	M	Monthly	Hard Copy (monthly) Soft Copy (weekly)
11	Management Audit reports of ROs	Central office/RO Inspection Dept.	M	Half Yearly / Yearly	Soft Copy

12	Management Audit reports of Nodal Audit Offices	Central office, Inspection Dept / Nodal Audit Offices	M	Half Yearly / Yearly	Soft Copy
13	Management Audit reports of CO Departments	Central office, Inspection dept/Concerned Depts.	M	6M/12M/18 M depending on risk perception	Soft Copy at Inspection Dept/ hard copy at user Dept.

B. <u>Records to be preserved for TEN years</u>

14	RBIA Inspection reports of Branches	Branch/RO/Inspection Dept Inspectorate/Central office, Inspection Dept.***	M	9M/12M/15 M/18M depending on risk perception	Soft copy in eTHIC server and hard copy at Inspectorate***
15	RBI Inspection reports of Branches and Regional Offices	Branch	M	As and When Conducted by RBI	Hard Copy
16	Migration Audit report	IS Audit Cell, CO	M	As and When Conducte d	Hard & Soft Copy

<u>INFORMATION SECURITY DEPT:</u>

Sl. No.	Records to be preserved	Period of Preservation	Risk Profiling
1	IS Security Committee, Architecture Committee, any other Committee notes, minutes submitted to Board / Top Management	Permanently	M
2	Board Notes / Top Management notes	Permanently	M
3	Information Security Policy / Procedures / Guidelines	Permanently	M

4	Cyber Security Policy / Procedures	Permanently	M
5	Cyber crisis management plan	Permanently	H
6	Day to day official documents	Permanently	M
7	SLA (Service Level Agreement)	Permanently	H
8	NDA (Non-disclosure Agreement)	Permanently	H
9	Purchase Orders	Permanently	M
10	RBI and other regulatory related correspondence document, circulars, advisories	Permanently	M
11	Department circulars	Permanently	M
12	Standard Operating Procedures	Permanently	M

DIGITAL BANKING DEPT:

Sl. No.	Records to be preserved	Period of Preservation	Risk Profiling
1	Budget Utilization Register	3 Years	M
2	All Miscellaneous reports, all MIS Reports	3 Years	M
3	SMS Logs	3 Years	M
4	Purchase Order Register/file	5 Years	M
5	Bills Payment Register	5 Years	M
6	P & L Register	5 Years	H
7	Sanction Note file	5 Years	H
8	CO Dept / RO Correspondence file	5 Years	M
9	RO Sanction file	5 Years	M
10	AMC & ATS files and related documents, after completion of contracts	5 Years	M
11	Miscellaneous file	5 Years	M
12	All Office Notes put up to GM/ED/MD&CEO	5 Years	H
14	Correspondence with ZO/RO/Branches, RBI/DFS, Vendors	8 Years	M

15	Complaint register	10 Years	M
16	Service Level Agreements and Non-Disclosure Agreements, after completion of contracts	10 Years	H
17	Project Files of completed projects	Permanently	H
18	Media for released products	Permanently	H
19	Board Notes	Permanently	H
20	All Audit Reports (Internal & External)	Permanently	H
21	Policies / SOP	Permanently	H
22	Desktop backup register	Permanently	H

CREDIT CARD DEPARTMENT:

Sl.No.	Records to be preserved	Period of Preservation	Risk Profiling
1	Correspondence from Regional Offices	10 Years	M
2	Staff matters/ Commission file	10 Years	M
3	BOD / ITD / TBD / Board Services file	Permanently	M
4	Chairman 's Sect/ ED sect/ Board services file	Permanently	H
5	RBI correspondence / office note-files	Permanently	M
6	Finance Ministry correspondence –files	Permanently	M
7	Inspection Progress Report	10 Years	M
8	Inspection file/ Statutory Audit/ Concurrent Audit	Permanently	M
9	Board Notes file/ schemes files	Permanently	M
10	Credit Card Centre- file	10 Years	M

RETAIL BANKING DEPARTMENT:

Sl.No.	Records to be preserved	Period of Preservation	Risk Profiling
1	Correspondence on complaints (after disposal of the complaint)	10 Years	M
2	Correspondence with Regional Office on clarifications sought on scheme related queries	5 Years	M
3	Loan Proposal / Sanction (after the closure)	5 Years	M
4	Leave Records / Attendance Register	Permanently	M
5	Statistical Data reported to other Departments	5 Years	M
6	Correspondence on Customer complaints received through Ministry/Other Regulators (after disposal of the complaints)	10 Years	M
7	General correspondence with Regional Offices/Branches	5 Years	M
8	BA/RBI/MOF communications file	5 Years	M
9	Statistical Data reported to IBA/RBI/NHB/SLBC/MOF and other Regulators	5 Years	M
10	Scheme formation –files	Permanently	M
11	Files related to sanctions advised to RO/ZOs on concessions/relaxation in scheme norms – Account specific actions -After Closure	5 Years	M
12	Files related to Subsidy received from Government/Other Nodal Agencies	10 Years	M
13	HLCC(GM)/HLLCC(ED)/CAC Notes	10 Years	H
14	RBI/IBA/NHB/MOF & Other Regulator's Correspondence File	5 Years	H
15	Board Notes	Permanently	H
16	Circulars Issued Files	Permanently	M

INDUSTRIAL RELATIONS DEPARTMENT:

Sl.No.	Records to be preserved	Period of Preservation	Risk Profiling
1	Staff committee meeting files	3 Years	M
2	General Correspondence	3 Years	M
3	All miscellaneous reports	3 Years	M
4	Inward/Outward Register (All Departments)	5 Years	M
5	Bio-metric reports	5 Years	M
6	Statistical Data reported to other Departments	5 Years	M
7	Compliance Certificate	5 Years	M
8	RBS return	5 Years	M
9	IR Clearance File	5 Years	H
10	General correspondence with Regional Offices	5 Years	M
11	Ghosh Committee recommendations	5 Years	M
12	IBA/RBI/MOF communications file	5 Years	H
13	All Correspondence with RO / Branches	5 Years	M
14	Statistical Data reported to IBA/RBI/NHB/SLBC/MOF and other regulators	5 Years	M
15	Guidelines / directives from ministry of finance/IBA	5 Years	M
16	Sanction note file	5 Years	H
17	Office Notes	5 Years	H
18	Legal Opinion of General Nature	5 Years	M
19	Misc. matters of all Regions	5 Years	M
20	NOC for availing loans from other banks / institutions register	5 Years	M
21	Sports files- General expenses	8 Years	H
22	Goiporia Committee Recommendations	10 Years	M

23	Standard Operating Procedures	10 Years	M
24	Concurrent Audit reports of CO Departments	10 Years	M
25	IS Audit reports of CO Departments	10 Years	M
26	Reply to RTI queries	10 Years	H
27	Management Audit reports	10 Years	M
28	Review Notes put up to ED/MD & CEO	13 Years	H
29	All Audit Reports (Internal & External)	13 Years	M
30	Circulars issued by CVC/Ministry/RBI/IBA etc., related to Vigilance Department.	Permanently	M
31	Circulars issued register	Permanently	M
32	Registers for voluntary retirement	Permanently	H
33	Registers: Department/ Voluntary retirement /Special Leave/ Disciplinary authority/Clerical officers/ Sub-staff	Permanently	H
34	Letter of voluntary cessation of employment	Permanently	H
35	Record of Terminations (box files) for all regions	Permanently	H
36	Returns relating to Movable/Immovable properties of staff members	Permanently	H
37	Appellate Authority Order Register	Permanently	H
38	Files related to disciplinary proceedings	Permanently	H
39	Files related to sabattical leave, permission accorded for employment after retirement, clearances for leaving abroad etc.	Permanently	H
40	Files relating to Vigilance & non-vigilance cases of employees	Permanently	H

41	Suspension orders, charge sheets, original orders, appellate orders and review orders issued to the employees.	Permanently	H
42	Appeal papers	Permanently	H
43	Appellate Orders	Permanently	H
44	Files related to quarterly compliance	Permanently	H
45	Board Related Files	Permanently	H
46	Board Notes relating to various policies and Schemes	Permanently	H

AGRICULTURE & RURAL INTIATIVES DEPARTMENT & FINANCIAL INCLUSION:

Sl.No.	Records to be preserved	Period of Preservation	Risk Profiling
1	Review of performance under various Schemes	3 Years	M
2	Review of BC performance and BC Office note, after termination as it is looking after CBC	3 Years	M
3	Registers/Reports/Files Loan Proposal Register	5 Years	M
4	Internal / External Training – Correspondence Seminars / Programmers / Original Training / Intensive Training /Work undertaken by Students and Apprentice training related file	5 Years	H
5	Files relating to ad-hoc references / Miscellaneous file	5 Years	M
6	SHG Linkage Proposals (after the closure)	5 Years	M
7	Suspense and Sundry Creditors Review	5 Years	M
8	Regional Rural Banks Board Minutes and Agenda notes	5 Years	M
9	RBS return	5 Years	M

10	Notes places to PRMC, BPRC etc	5 Years	M
11	Creation of GL code (file)	5 Years	M
12	Business/ Corporate card/third party letter	5 Years	M
13	Financial Disclosures data/outsourcing reports submitted to RBI/BSMD etc.,	5 Years	M
14	All MOUs, after expiry	5 Years	M
15	Office Notes	5 Years	M
16	Loan Related: (Five years after closure of loan) • Loan proposal /sanction (after the closure) • Loan Proposal / Sanction (after the closure)	5 Years	M
17	Sanction note file	5 Years	M
18	Claim Papers of accounts of deceased customers	8 Years	M
19	Files related to sanctions advised to RO/ZOs on concessions/relaxation in scheme norms - Account specific actions	10 Years	M
20	Banking Ombudsman related Correspondences	10 Years	M
21	Office Copies of returns submitted to RBI/ NABARD/DFS	10 Years	M
22	Reimbursement claims submitted to NABARD / STATE GOVT. / CENTRAL GOVT.	10 Years	M
23	RBI/Indian Banks Association/NHB/MOF/GOI and other regulatory related correspondence documents	10 Years	M
24	NABARD Refinance Register	10 Years	M
25	Files related to Subsidy received from Government/Other Nodal Agencies	10 Years	M

26	HLCC(GM)/HLLCC(ED)/CAC Notes	10 Years	M
27	Standard Operating Procedures	10 Years	M
28	All circulars related to any matters other than listed under permanent head.	10 Years	M
29	All Audit Reports (Internal & External)	13 Years	M
30	**Loan Related Files** **Non-Staff:** ▪ All files / records relating to existing borrower accounts ▪ All borrower files ▪ Credit Files List of Willful Defaulters ▪ List of Non-Co-Operative Borrowers ▪ List of Fraud Declared NPA accounts ▪ All documents, records and files	Permanently	M
31	**Office Notes:** ▪ Office notes relating to policy decisions and guidelines, procedures/ background papers in respect of permanent circulars ▪ Office Notes, files, roster (with regular changes and updation).	Permanently	M
32	**Board related files:** • Agendas, minutes, action and ATR of all Risk Management Committee meetings i.e. ORMC, CPC, ALCO, PRMC, TMC, AC-ED & AC-GM (CO) etc. • RMCB, ACB, MCB and Board approved Notes relating to	Permanently	M

	Policies, Studies, information notes etc., • All review notes put up to ACB / Management Committee of Board / Board / GM Committees • Board Notes relate to various schemes •Board Notes relating to Performance Budgeting, Credit Planning, Branch Expansion, Costing and MOU cell •Copies of all recorded Board Notes		

CUSTOMER SERVICE DEPARTMENT:

Sl.No.	Records to be preserved	Period of Preservation	Risk Profiling	Remarks
1	Seminar on Customer Service	3 Years	M	
2	Files/Records of Customer Service Cell at Regional Offices	5 Years	H	
3	Files/Records of Customer Meeting conducted	5 Years	M	
4	Files/Records about Customer Education	5 Years	M	
5	Complaints received / settled	5 Years	M	
6	Files/Records of Customer service in Banks	5 Years	M	Only if documented
7	Files/Records of Calendar of reviews	5 Years	M	Only if documented
8	Settlement of complaints / Staff lapses	5 Years	M	
9	Survey on Customer Service	5 Years	M	
10	Executive Meeting with RBI	5 Years	M	Only if documented
11	Analysis of complaints	5 Years	M	
12	Action taken on RBI Governor's Meeting	5 Years	M	
13	Monitoring implementation of instructions of Government and Reserve Bank of India	5 Years	M	
14	Management information reports	5 Years	M	
15	Grievance cell/ Redressal meeting	5 Years	M	
16	DPG (Directorate of Public Grievances) Complaints	5 Years	M	

HUMAN RESOURCES MANAGEMENT DEPT:

Sl.No.	Records to be preserved	Period of Preservation	Risk Profiling	Remarks
1	Mails and Courier	5 Years	M	
2	Dispatch Register	5 Years	M	
3	Misc. matters of all Regions	5 Years	M	
4	Complaints / Grievance Register	5 Years	M	Electronically / Online Portal
5	Other Bank Correspondence	5 Years	M	
6	Statement / Registers relating to Staff leave matters	5 Years	M	Electronically / Online Portal
7	Passport's clearances issued	5 Years	M	Electronically / Online
8	IR Clearance File	5 Years	M	ICPS Online
9	All staff related files	Permanently	H	

COMPLIANCE DEPARTMENT:

Sl.No.	Records to be preserved	Period of Preservation	Risk Profiling
1	General Correspondence	10 Years	M
2	All miscellaneous reports	5 Years	M
3	Bio-metric reports	5 Years	M
4	Letter Received Register	Permanently	M
5	Misc. matters of all Regions	5 Years	M
6	General correspondence with Regional Offices	10 Years	M
7	Correspondence / Miscellaneous files related to staff matters.	5 Years	M

8	IBA/RBI/MOF communications file	5 Years	M
9	Office Notes to GM	5 Years	M
10	Bills payment register / files	Permanently	M
11	Annual Financial inspection by RBI	10 Years	M
12	RBI/Indian Banks Association/NHB/MOF/GOI and other regulatory related correspondence documents	10 Years	M
13	RBI related: ▪ Reply submitted to RBS/RBI/AFI. ▪ Correspondence Files with RBI / IBA ▪ RBI Automated Data Flow – Correspondence File ▪ RBI and Ministry of Finance directives – files ▪ All DSB returns submitted to RBI ▪ RBI circulars	Permanently	H
14	Policy clearances	Permanently	H
15	Board related files: • Agendas, minutes, action and ATR of all Risk Management Committee meetings i.e. ORMC, CPC, ALCO, PRMC, TMC, AC-ED & AC-GM (CO) etc. • RMCB, ACB, MCB and Board approved Notes relating to Policies, Studies, information notes etc., • All review notes put up to ACB / Management Committee of Board / Board / GM Committees • Copies of all recorded Board Notes • Review Notes put up to various Authorities including Board	Permanently	H

STAFF ACCOUNTABILITY CELL:

Sl.No.	Records to be preserved	Period of Preservation	Risk Profiling
1	First Vetting Committee Note	Permanently	H
2	Second Vetting Committee Note	Permanently	H
3	Tri - column Note	Permanently	H
4	SAC Profile	Permanently	H
5	SAC Minutes	Permanently	H
6	Minutes Remarks Sheet	Permanently	H
7	SAC Files – Upgraded / Closed by Vetting Committee	Permanently	H
8	SAC Files - Concurred and Returned by Vigilance Dept	Permanently	H

CDAC:

Sl.No.	Records to be preserved	Period of Preservation	Risk Profiling
1	All Inward and Outward Registars duly recording the inflow and outflow of files and other correspondences	Permanently	H
2	All Data including (MIS to Top Management & CVO, Returns to RBI & DFS) and files pertaining to all Disciplinary cases (Both Vigilance and Non-Vigilance)	Permanently	H
3	Copies of Charge Sheets	Permanently	H
4	Copies of Disciplinary Authority's Final Orders	Permanently	H
5	Appeal Files and related Appellate Orders	Permanently	H

6	Review Files and related Review Orders	Permanently	H
7	All 17 A and 19 correspondences, Sanctions Related to CBI Investigation and Prosecution files	Permanently	H
8	All court cases challenging Bank's Disciplinary Proceedings and orders and related files	Permanently	H

MARKETING DEPT:

Sl.No.	Records to be preserved	Period of Preservation	Risk Profiling
1	Scheme wise/Interest Rate correspondence with Regional Offices/ Branches	5 years	M
2	IBA communications file	5 years	M
3	Scheme formation –files	Permanently	H
4	Interest Rate file	Permanently	H
5	Interest / Board Notes File	Permanently	H
6	RBI circulars file	Permanently	H

INTERNATIONAL DEPT:

Sl.No.	Records to be preserved	Period of Preservation	Risk Profiling
1	Correspondence pertaining to repatriation of members	5 years	M
2	Various MIS Reports	5 Years	M
3	Review of Concurrent Audit report of Overseas Branches	5 years	H

4	Board Notes	Permanently	H
5	Credit Files	Permanently	H
6	Policies	Permanently	H

GOVERNMENT ACCOUNTS DEPT:

The records pertaining to Government transactions should be destroyed only after getting prior permission from Government Accounts Dept. The period for which the records should be preserved is shown below for the information of branches.

- Scheme for acceptance of Income and other Direct Taxes
- Scheme for collection of Central Excise, Customs and other dues.
- Scheme for collection of State revenue
- All forms & ledgers relating to Small Savings Schemes, National Pension Scheme, Bond ledger accounts
- Any other collection /payments for State /Central government handled by the Bank as an agency Bank.
- Print Payment Advice/Electronic Payment Advice (PPA/EPA) of PFMS transactions

Sl.No	***Record/Register***	***Form No.***	***Period of preservation (in years)***
	Part: A: Scroll and Summary Records		
	Receipt Scroll	PSB.7 (F421/471)	Ten
2	Payment Scroll	PSB.7	Ten
3	Daily Summary	PSB.8(receipts)	Three
4	Daily Summary	PSB.8 (payments)	Three
5	Daily Record of collection	PSB.9	Three
6	Advice of transaction of Focal Point Branch	PSB.10	Three

Any other records relating to Government Business, the preservation period is till elimination or the period mentioned above, whichever is later.

Records prescribed under Scheme for payment of Central/ Civil/ Defence/

Railways/ State Government Pension

Sl.No	*Record/Register*	*Form No.*	*Period of preservation (in years)*
1.	Application for withdrawal of pension	F.429/472/489	Permanent
2.	Application for family pension	F.432/475	Permanent
3.	Index Register for Pension payment (Link branch)	F.438/478/493	Permanent
4.	Index Register (Link/Paying Branch)	F.437/478/493	Permanent
5.	Pension Payment Account Register	F.436/479/493	Twenty Five
6.	Pension Payment Scroll	F.434/489/491	Five
7.	Summary Sheets-Link Branch	F.434/481/494	Five

Any other records relating to Central/State Government Pension, the preservation period is till elimination or the period mentioned above, whichever is later.

Record to be preserved permanently and under no circumstances to be destroyed unless authorized.

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.

- Records 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, shallbe 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 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 orwhen 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.,

PART D – PRESERVATION PERIOD OF RECORDS - FOR ROs/BRANCHES

Sl.No.	Records to be preserved	Period of Preservation	Risk Profiling	Mode of Keeping
1	Account opening forms of Savings Bank, Current account, Term Deposits and all other accounts along with KYC and OVDs	Permanently	H	Physical
2	Powers of attorney (Current and Savings Bank)	Permanently	H	Physical
3	Register for Power of Attorney, Succession Certificates, Death Certificates etc.	Permanently	H	Physical
4	Specimen Signature books	Permanently	H	Physical
5	Register for Nomination of deposits	Permanently	H	Physical
6	Loans, Cash Credits, Overdraft Sanction Registers which contain particulars of Title deeds relating to accounts which are in force	Permanently	H	Physical
7	Register of Mortgages and Charges	Permanently	H	Physical
8	Safe Deposit Locker Register / Agreements	Permanently	H	Physical
9	Account opening forms, inventories, prepared in respect of articles in Safe Custody and Safety Lockers and nomination forms	Permanently	H	Physical
10	All records relating to cash transactions where forged or counterfeit Currency Notes used with transaction details	Permanently	H	Physical
11	Key Movement Register	Permanently	H	Physical
12	Staff Files	Permanently	H	Physical (Branches / Regional Offices)
13	Allocation / Office Orders	Permanently	H	Physical
14	Files related to Furniture / Fixtures	Permanently	H	Physical

15	Premises and properties files and records	Permanently	M	Physical
16	Indemnity Bonds	Permanently	M	Physical
17	ATM Card/Debit Card issue – Registers/ Applications	Permanently	M	Physical
18	Request for duplicate PIN	Permanently	M	Physical
19	Internet banking – New Regn & other requests	Permanently	M	Physical
20	Claim application on account of deceased Non-Resident (Ordinary)/ Non Resident (External)/ FCNR(B) account holders	Permanently	M	Physical (Branches / Regional Offices)
21	Records pertaining to unpaid Export Bills along with correspondence	Permanently	M	Physical
22	EM Register	Permanently	M	Physical
23	Jewel Appraiser's File	Permanently	M	Physical (Regional Office)
24	Death Claim Settlements	Permanently	M	Physical (Branches / Regional Offices)
25	Insurance claim lodged register in case of deceased customers	Permanently	M	Physical (Branches / Regional Offices)
26	Records / Files of court orders and Powers of Attorney	Permanently	M	Physical (Branches / Regional Offices)
27	Records / Files pertaining to empanelment of valuers / advocates incl the documents submitted for empanelment and also the decision/ permission letter of the Competent Authority with regard to the said Empanelment.	Permanently	M	Physical (Regional Office)
28	Record register & Register indicating Records to be held in Electronic Form	Permanently	M	Physical (Branches / Regional Offices)
29	Slips, Cheques and voucher relating to SB / CD / CC / DDs, FDs and all other deposits, loans, overdrafts, bills etc.	10 Years	M	Physical

30	NRO /NRE /FCNR/RFC and Non-Resident Deposit forms	10 Years	M	Physical
31	Register for Nomination of deposits	10 Years	M	Physical
32	Files related to Accounts held with other Banks	10 Years	M	Physical (Branches / Regional Offices)
33	Files/Register related to auction of goods and other securities such as gold etc.	10 Years	M	Physical
34	Cash Remittance Register	10 Years	M	Physical
35	Accounts Opened / Closed Register	10 Years	M	Physical
36	Account opening forms, inventories, prepared in respect of articles in Safe Custody and Safety Lockers and nomination forms	10 Years	M	Physical
37	Safe Deposit Locker Register / Agreements	10 Years	M	Physical
38	Key Register	10 Years	M	Physical
39	Slips, Cheques and voucher relating to DDs, FDs and all other deposits, loans, overdrafts, bills etc	10 Years	M	Physical
40	Debit/Credit/ Prepaid card Issue Register at branches	10 Years	M	Physical
41	The application forms and other request forms pertaining to Sovereign Gold Bond Scheme.	10 Years	M	Physical
42	Premature redemption request of Sovereign Gold Bond scheme from the date of payment of proceeds.	10 Years	M	Physical
43	All Records related to suspicious transactions, whether or not made in cash and by way of as mentioned in the Rules.	10 Years	M	Physical
44	Register of sanctions, TOD sanctions/ratification.	10 Years	H	Physical (Branches / Regional Offices)

45	Security Documents of Loans (10 Years from the date of closure of the account)	10 Years	H	Physical
46	Original Bank Guarantee	10 Years	H	Physical
47	Daily Transaction Vouchers	10 Years	H	Physical
48	Vouchers bundled and stitched	10 Years	H	Physical
49	Applications for PPF Accounts (10 years after closure of the account)	10 Years	H	Physical
50	Documents pertaining to SOCIAL SECURITY SCHEMES – for Insurance and Pension: a. Pradhan Mantri Jeevan Jyothi Bima Yojana (PMJBY) b. Pradhan Mantri Jan Suraksha Bima Yojana (PMSBY) c. Atal Pension Yojana (APY)	10 Years	H	Physical
51	Nostro Bank mirrors, Forward Merchant contract registers, EEFC/RFC/FCNR(B).	10 Years	H	Physical
52	Claim files after the date of settling	10 Years	H	Physical
53	BGs issued / invoked register	10 Years	H	Physical
54	Loans, Advances, Cash Credit and Overdraft Registers	10 Years	H	Physical
55	Safe in and Safe out Registers (Securities kept in and taken out) - Safe Custody	10 Years	H	Physical
56	Mandate Forms for Current / Savings account (Permanent till authorization is in force)	10 Years	H	Physical
57	Files/Letters/Communications related to Drafts and Deposit Receipts/other security items lost	10 Years	H	Physical
58	Reconciliation statement for accounts held with other banks	10 Years	H	Physical
59	Enrollment form /Auto- debit authorization /Consent cum Declaration form in the	10 Years	H	Physical

	prescribed proforma, as required by LIC / other insurance company (10 years after closure of the account).			
60	Applications for Overdraft (loans/ advances)	10 Years	H	Physical
61	Closed files of Suit filed /writ petition/ consumer forum cases	10 Years	H	Physical
62	Cheques Requisition Slips / Requests	10 Years	H	Physical
62	Cheques Issued / Stopped, Returned Registers	10 Years	H	Physical
63	General Files related to correspondence from / to Local bodies / Govt Authorities	10 Years	M	Physical (Branches / Regional Offices)
64	Legal Opinions taken for other matters	10 Years	M	Physical (Branches / Regional Offices)
65	Letters of Credit - Application forms	10 Years	H	Physical
66	Inland letters of credit- opening forms	10 Years	H	Physical
67	Advice of Letters of Credit	10 Years	H	Physical
68	LIC of India Memorandum (Duplicate) & correspondence files	10 Years	M	Physical (Branches / Regional Offices)
69	Files of rejected loan proposals (incl all Govt Sponsored schemes)	10 Years	H	Physical (Branches / Regional Offices)
70	Drawing Power Register	10 Years	H	Physical
71	Inspection / Audit Reports	10 Years	H	Physical (Branches / Regional Offices)
72	Concurrent Auditor's Report	10 Years	H	Physical (Branches / Regional Offices)
73	Re-finance, Crop insurance, Settlement of Insurance & Other claims	8 Years	M	Physical

74	Documents pertaining to the NPA accounts settled under compromise settlement by the Bank.	8 Years	H	Physical (Branches / Regional Offices)
75	Loan Documents pertaining to the NPA accounts settled under Lok Adalat and related order/s	8 Years	H	Physical (Branches / Regional Offices)
76	Godown keys and insurance policies register	8 Years	H	Physical
77	Godown register measurement, inspection	8 Years	M	Physical
78	Field inspection reports	8 Years	M	Physical
79	Security items receive and release register	8 Years	H	Physical
80	Jewel Movement Register	8 Years	H	Physical
81	Staff Files (Correspondence) / Leave Statements	5 Years	M	Physical (Branches / Regional Offices)
82	Closed files of cases under Consumer Forum, Suits/ WPS	5 Years	M	Physical (Branches / Regional Offices)
83	No excess cash certificate	5 Years	M	Physical
84	Remittance dispatched and received registers.	5 Years	M	Physical
85	T A Bill, Medical Aid, Hospitalisation etc. files/ledgers	5 Years	M	Physical (Branches / Regional Offices)
86	General Charges Register	5 Years	M	Physical
87	Daily cash tally register – For CDMs	5 Years	M	Electronic
88	Bill realization letters received from collecting Bankers/ Branches	3 Years	M	Physical
89	Progress report of the branch/Branch Diary	3 Years	M	Physical
90	ATM Machine Complaint Register	3 Years	M	Physical
91	Register for ATM custodians for safe lock password change	3 Years	H	Physical
92	Request for claim for disputed transaction from Customers / Non – Customers	3 Years	H	Physical (Branches / Regional Offices)

93	Payment to customers for disputed transactions (Alternate Channels)	3 Years	H	Physical
94	Periodical statements submitted to various authorities	3 Years	H	Physical (Branches / Regional Offices)
95	Inspection Reports – Unit Visit / Other Securities	3 Years	H	Physical (Branches / Regional Offices)
96	Lease Deed of Premises / Quarters (3 years after the expiry of lease)	3 Years	H	Physical (Branches / Regional Offices)
97	Forms of nomination/ cancellation of PPF	3 Years	H	Physical
98	Premature redemption request of Sovereign Gold Bond scheme from the date of payment of proceeds.	3 Years	H	Physical
99	Bill realization letters received from collecting Bankers/ Branches	3 Years	H	Physical
100	Register for Computer consumables.	3 Years	H	Physical (Branches / Regional Offices)

Notwithstanding anything contained in this policy:

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.

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 Clientsof 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

Branch/RO/CO department must mandatorily take permission from General Manager (Law) prior to disposal of any record /document relating to any legal case /judicial case/ etc., Records not falling in any of the above categories shall be maintained for a period of ten (10) years from the date of cessation of the transactions with the client / customer.