Technology Guidelines for Retention and Destruction of Electronic Data

Introduction:

These guidelines aim at guiding the employees of the Bank on the types and sources of generation of electronic data and the manner of retention and destruction of the same. It is important to read the guidelines in conjunction with the "ICICI Bank Record Maintenance and Destruction Policy".

Digital/Electronic data in ICICI Bank can broadly be classified (but not limited to) into the following areas.

- Data generated in various Applications/Systems (business/transaction data & system data viz. trails/logs)
- Data generated through Emails
- Data generated through SMS alerts
- Data generated through promotional SMSes sent to customers
- Data generated through i-Core & Finone MIS
- Data generated and stored in Local machines (PCs, Laptops etc.)/end points
- Data generated & stored in file servers (Shared folders)

The following sections detail out how the data is proposed to be retained and destroyed in each of the above areas.

The data could be HOT, which means it is easily and immediately accessible. Such data may be available on the server infrastructure/inside the application or system and can easily be accessed from the front end or by execution of queries from backend.

The data could be COLD, wherein the data may be stored on external digital media (DV/CD ROMs), tapes or in a separate archival database etc. In case of COLD data, the period and the method of extraction will be more than the HOT data.

Data generated in various Applications/Systems

The Bank has many and varied systems/applications which enable/facilitate to perform Banking functions/activities. Data or information is generated in these applications/systems. Every application/system has an application owner and a business owner who would be responsible for managing, maintaining and destroying the data/information generated in these Applications/systems.

The storage, retention and purging of data is generally governed by the prevailing regulatory & other guidelines pertinent to the respective lines of business. In case of purging, it may also be dependent on the extent of linkages, an application has with other interfacing applications. "Data Retention and Purging Note", to be jointly defined by Compliance, Legal, Operations, Product team alongwith the respective business & technology owner of the application. In case of application logs which are generated at the Operating system level would be retained for a period depending on the nature of the application.

The note should also state the indicative time of retrieval in case of HOT or COLD data. Additionally, the "Data Retention and Purging Note" should also document the retention and purging period for the system data viz. logs or audit trails.

Based on this note, it is the joint responsibility of the Business & Technology owner to periodically carry out the data retention & purging.

Exceptions:

Limitations of the following nature would need to be handled as exceptions in case of access/restoration. This is an indicative list and not an exhaustive list.

- a technology limitation in restoring old data which has been stored on external media due to enhancements in backup technology or bad media

- vendor support not available,

- vendor out of business,

-product is not licensed to bank anymore and hence application not being accessible.

In case of such limitations, the Business Owner alongwith the Technology Owner has to formulate and document Plan of managing such data for future retrieval as well as deletion.

In case of application logs which are generated at the Operating system level would be retained for a period depending on the nature of the application.

Data generated through Emails

All e-mails created by individuals will be owned and protected by them, especially if they contain important/confidential information. In case of exigency, if any approvals have been obtained on e-mails and not vide i-Memo/i-Process, it is mandated that such approvals to be regularised by attaching as enclosures/attachments to i-Memo/i-Process approvals.

The Technology team maintains a copy of every email received and is saved in the central email archival system. These mails are only retained for regulatory purposes and are not provided to end users as email backup.

Further, emails which are generated by applications and sent through the Mass mailing system for example: Statement generation mails generated from i-Core are not retained and are also not backed up. SMTP (Simple Mail Transfer Protocol) logs for mass mailers are purged after 7 days and there is no backup for these logs.

Email destruction:

Emails will be retained as per Bank's policy (presently 10 years) from the date of origination.

Data generated through SMS alerts

SMS alerts generated and sent are retained for a period of three months from the date of origination.

Data generated through Promotional SMSes sent to customers

Promotional SMSes generated and sent to customers are retained for a period of three months from the date of origination. For analytical purposes these SMS texts may be stored upto a maximum period of three years.

Data generated through i-Core & Finone MIS

Various teams in the bank request for MIS reports on i-Core data. These reports are generated out of i-Core MIS server and are stored in a defined location. These reports are retained for a period of one week.

In case of Finone (App Processing System/CAS (Customer acquisition system). CAPS & LMS) MIS, the generated reports are also stored in a defined location. These reports are retained for a period of one week.

Data generated and stored in Local machines (PCs, Laptops etc.)/end points

The data generated on the user's machines could be of various forms i.e. Structured, unstructured, email, etc. The types of data would range from data extracted from databases, reports, MIS for the Bank's Senior Management to scanned documents or agreements or images. It would be the responsibility of the individual users to ensure the integrity and confidentiality of the data that has been stored on the Bank's assets (local machines). Users shall personally take care of critical and important files as no backup is being taken for the data stored on end-user machine. It is recommended that users should keep only the data relevant to their work profile on their PCs. Additionally, any critical data which may be needed in future should be moved to the common folders.

Data generated and stored in file servers(shared folders)

During the day to day functioning, users may generate data such as important reports, MIS for the Bank's Senior Management, scanned documents such as agreements. Such documents also need to be retained & destroyed as per the policy. For retention of such critical data, every department has been provided with a storage location, commonly referred as file server (shared folder). The access to this storage location is managed by the respective departments internally. It would be the responsibility of the individuals to ensure the availability of critical data on file servers. It would be the responsibility of every individual and their Department Heads to manage the activities around the preservation and destruction of data in line with the policy, on these file servers.

File servers will be backed up as per the extant guidelines.

Backup policy for file servers

Backup Policy	**Type**	**Retention period**
Daily	Incremental	1 Week
Weekly	Full	1 Month

Data restoration scenario limitations:

As the backup jobs are scheduled in the night, any data which is created during the day and if the data gets deleted the same day due to corruption, human error or intentionally or due to a hardware failure, this data cannot be recovered as it was outside the scheduled backup window.