Record Retention, Disposal and User Information Policy

DOCUMENT HISTORY

Document Name	Record Retention, Disposal and Cardholder Information Privacy Policy
Document Reference Number	Version 1.0
Classification	Internal
Version Number	V 1.0
Date	30/04/2024
Reviewed by	IT Team
Approved by	Board of Directors

REVISION HISTORY

Date	Version	Description	Created by
30/04/2024	V 1.0	First Release	IT Team

1. Introduction

The Reserve Bank of India vide its Notification Ref. No. RBI/2022-23/111 DOR.CRE.REC.66/21.07.001/2022-23 dated September 02, 2024 viz. Guidelines on Digital Lending as amended from time to time, advised to the implement a clear Policy guidelines regarding the storage of customer data including the type of data that can be stored, the length of time for which data can be stored, restrictions on the use of data, data destruction protocol, standards for handling security breach, *etc.*.

The Record Retention Policy aims at streamlining this and ensuring the smooth functioning of the Company.

Data backup and recovery form a core component of our disaster recovery strategy. To align with Akara's mandated security standards, it is crucial to maintain an optimal data retention strategy. This strategy supports our operational efficacy and meets legal, regulatory, or donor requirements, or provides proof in disputes.

2. Purpose

This protocol aims to manage data in compliance with Akara's strategic, legal, and regulatory frameworks, ensuring data confidentiality, integrity, and availability. It outlines the practices for data preservation according to commercial and industrial needs, ensuring data is safeguarded against damage, loss, or alteration and systematically retained to facilitate easy access in a suitable format for end-users.

Its core aspect is as follows:

a. Nature and types of documents to be preserved/archived and retrieved.
b. Duration and circumstances under which they must be preserved.
c. Security and confidentiality of these records/documents.
d. Mode of destruction including but not limited to electronic and physical.

3. Scope

This protocol governs all information, electronic and computing devices, and network resources used in Akara's operations. It applies to all employees, contractors, vendors, and agents who use these resources. It encompasses all records, whether digital or physical.

4. Duties and Responsibilities

Roles	Responsibilities
All Users	Adhere to the policy guidelines.
IT Team	Implement and oversee the record management and destruction protocols.

Business Units	Determine data retention periods based on business needs and regulatory requirements.
Information Security Team	Ensure policy compliance, handle security incidents, and conduct periodic audits.

5. Policy Provisions

5.1. Personal Identifiable Information

5.1.1. Personal Data: Special considerations are required for managing Personally Identifiable Information (PII), including stringent processing limitations and clear logging and deletion practices post-requirement.

5.1.2. Record Maintenance and Security: Establish and maintain records to demonstrate compliance and efficient operations, ensuring they meet all relevant standards and are protected during storage, transmission, and disposal.

5.1.3. Data Restoration and Backup: Manage data restoration processes and conduct regular audits of backup practices to ensure compliance and data integrity.

5.1.4. Data Retention and Disposal: Define clear guidelines for data retention based on business, legal, and contractual needs and ensure secure destruction of data once it is no longer required.

5.2. Record Maintenance

5.2.1. It is essential for all users to categorize the information assets according to Akara's classification and labeling standards, ensuring robust controls are implemented to block unauthorized access.

5.2.2. Records must be created and preserved to demonstrate adherence to operational and compliance standards

5.2.3. Records must align with legal, regulatory, and organizational policies, and fulfill contractual duties throughout their lifecycle including storage, transmission, and eventual disposal.

5.2.4. Specific protocols should be established for the identification, safeguarding, retrieval, maintenance, and elimination of records

5.2.5. Each record must include a unique Document/Record ID and a descriptive Record Name for identification.

5.3. Record Security and Restoration

5.3.1. Records shall be retained as per retention requirements.

5.3.2. Records need to be kept in line with established retention guidelines and secured appropriately.

5.3.3. Physical documents should be stored in lockable, and where possible, fireproof storage units.

5.3.4. Digital records must be maintained on secure, designated drives with controlled access to prevent unauthorized entry.

5.3.5. Detailed logs must be maintained for any use or alteration of stored data.

5.3.6. Access lists for personnel who handle or have access to these records should be updated and reviewed quarterly or upon changes in staff or protocol.

5.3.7. Restorations are initially performed on a standby system before being transferred to the operational system, with direct restorations being an exception that requires explicit authorization

5.3.8. While restoring the files and directories, it shall be ensured that access permissions are not changed or corrected after restoration is complete.

5.3.9. The Backup Administrator is responsible for logging details such as restoration date, time, and storage specifics.

5.4. Record Retention

5.4.1. The retention timeframe dictates the minimum duration records must be preserved to meet business, legal, regulatory, and contractual needs.

5.4.2. After this period, records may be retained longer if justified by business or legal needs, with the same level of security maintained.

5.4.3. Changes to retention periods must be documented with reasons.

5.4.4. Regular audits will be conducted to identify data that surpasses retention needs and to ensure its secure deletion.

5.4.5. The retention rules that apply to Akara records are outlined in the Section 5.6.

The indicative list for class of documents and the time period for which it is required to be maintained is provided in **Schedule I and Schedule II**.

5.5. Record Disposal

5.5.1. Upon meeting their retention timeline, records must be destroyed securely.

5.5.2. The process for identifying records for disposal should be systematic, embedded in daily operations, and compliant with the organization's protocols.

5.5.3. Disposal actions are contingent on the records being obsolete, not needed for ongoing or impending legal actions, and not required to fulfill any legal, regulatory, or contractual obligations.

5.5.4. Secure destruction methods, adhering to standards like DoD 5220.22-M or NIST SP 800-88, will be employed

5.5.5. Electronic media will be wiped clean prior to disposal. A designated IT team member will oversee the destruction of data storage devices.

5.5.6. Hard drives will be degaussed and then handed over to certified disposal firms.

5.5.7. A destruction certificate from the disposal company will be secured, and a detailed log of the disposal process will be maintained.

5.6. Custody of Documents:

- Subject to the Applicable Law, the custody of the documents shall be with the Authorised Person. Where the Authorised Person tenders resignation such Person shall hand over all the relevant documents, lock and key, access control or password, or USB storage drives/pen drive/hard disk/one drive data/other storage devices or such other documents and devices in his possession under the Policy.

- Functional Heads and/or one level below the Functional Head, shall be responsible for ensuring compliance of this Policy, as related to records in their possession, custody or control.

6. Incident Priority & Corresponding Response Timelines:

Severity	Description	Response timelines	Probable Incidents
Low	The severity would threaten the efficiency or effectiveness of the services But does not impact client delivery / security measures like isolated anti-virus alert, spam E-Mail, outlook issues like multiple mails being shot at one instance without anybody's notice, etc...	Incident should be acknowledged and correction to be initiated within 8 hours. Corrective action timelines will be determined on a case to case basis.	Breaches detected in Information Security Policy having low impact to the organization – like, systems not complying with information security standards and controls Chain E-Mail and Internet abuse detected on a non-criminal nature – for example visiting prohibited sites. Virus alerts generated on Desktop / Laptop (not more than 5 systems). Semi critical files detected to be deleted by a user. Password sharing with unauthorized persons
Medium	The severity would threaten the delivery of services temporarily and could create minor impact on client delivery like E-Mail/internet down for few hours…	Incident to be acknowledged and correction to be initiated within 4 hours. Initiation of corrective action also to be done within 4 hours.	Breaches detected in Information Security Policy having medium impact to the organization – like, systems not complying with information security standards and controls Chain E-Mail and Internet abuse detected on a non-criminal nature – for example visiting prohibited sites. Virus alerts generated on Desktop / Laptop (not more than 5 systems). Semi critical files detected to be deleted by a user. Password sharing with unauthorized persons
High	The severity would threaten the provision of services, causing major impact to client delivery / security measures like any critical server down for a day, report could not be generated…	The incident to be acknowledged and correction to be initiated within 2 hours. Initiation of corrective action also to be done within 2 hours.	Breach of information security policy creating severe impact to the organization. Denial of service attacks that cause significant downtime. Reported loss of highly confidential electronic information like sensitive reports or files. Identification of unauthorized changes being made to the files / databases. Virus found in Server or virus outbreak spreading to all user Desktop/Laptop. Trojans or malicious code found on systems that impacts on the availability of systems or

			theft of information like key loggers, mass mailers, denial of service tools etc. Confidential E-Mail sent to unauthorized person. Defacing or other hacking activities on external web sites example the pages changed are not easily accessible and visible to the public. Loss of IT assets containing sensitive information. Detection of unauthorized wireless access points.
Critical	The severity would threaten the provision of services, causing major impact to client delivery / security measures like any critical server down for more than a day, report could not be generated…	The incident to be acknowledged and correction to be initiated within 1 hour. Initiation of corrective action also to be done within 1 hour.	Internet worm affecting multiple network, causing major downtime. Incidents that could lead to major damage to the reputation of the organization – like leaked confidential documents; loss of client data; disclosure of sensitive information (financial, personal etc.)

7. Amendments to the Policy

This policy may be updated or amended from time to time to maintain compliance with legal standards and best practices. All stakeholders will be notified of significant changes.

8. Related Policy

- Legal and Regulatory Compliance Policy

9. Abbreviations

- IT – Information Technology
- HR – Human Resource
- SAD – Sensitive Authentication Data
- PIN – Personal Identification Number
- CVV – Card Verification Value
- CD – Compact Disc
- DVD – Digital Versatile Disc
- CDE – Cardholder Data Environment
- NIST – National Institute of Standard and Technology
- ISO 27001:2022 – Information Security Management System

10. References

- ISO 27001:2022

SCHEDULE I

Sl. No.	Name of Documents	Period specified under the law
1	All Documents and Information as originally filed with the Registrar of Companies for Incorporation of Company *[Section 7(1)]*.	Permanent
2	Memorandum and Articles of Association, duly updatedfrom time to time *[Section 15]*	Permanent
3	Register of Renewed and Duplicate Share Certificate(Form SH-2) *[Section 46 & Rule 6(3) of Chapter IV]*	Permanent
4	Books and documents relating to the issue of sharecertificates including blank forms of share certificates *[Section 46 and Rule 7 of Chapter IV]*	Thirty years. But in case of disputed cases, permanently
5	Register of Transfer and Transmission *[Section 56]*	Permanent
6	Register of Charge (Form CHG-7) *[Section 85 & Rule 10 of Chapter VI]*	Permanent
7	Register of Members including foreign register, if required (with index of names if no. of members is notless than 50) *(Form MGT-1)* and Record of Beneficial Owners	Permanent
8	Minutes of Board Meeting and other Committee Meetings of the Board and resolutions passed by Circulation Minutes of the General Meetings of class of shareholders / creditors or resolutions passed by way of postalballots. *[Section 118, 119 & Rule 25 of Chapter VII]* Books and Papers of Amalgamated Companies *[Section 239]*. Minutes of all Meetings of the transferor company, as handed over to the transferee company. *[SS-1 & SS-2]*	Permanent
9	Register of Investments made by Company not held in its own name (*Form MBP-3*) *[Section 187 & Rule 14 of Chapter XII]*	Permanent
10	Instrument creating Charge or Modification thereof *[Section85 and Rule 10 of Chapter VI]*	Eight years from the date of Satisfaction of Charge
11	Register of Debenture Holders or other security holders(*Form MGT-2*) *[Section 88 (1) (a) and Rule 4,5,6 of Chapter VII]*	Eight years after the redemption of

		debentures or other security holders
12	Books of Accounts and Balance Sheet and Profit and Loss Statement [*Section 128(5)*]	Eight years from the date of filing with the Registrar
13	Notice of Interest by Directors and Key ManagerialPersonnel *[Section 184(1) and Rule 9(3) of Chapter XII]*	Eight years from the close of relevant financial year
14	Attendance Register of Meetings of the Board and Committees *[SS-1 – Clause 4.1.7]*	Eight years from the close of the relevant financial year
15	Office copies of Notices, Agenda, Notes on Agenda and other related papers of the transferor company, as handed over to the transferee company *[SS-1 – Clause 8.2]*	At least eight financial years
16	Office copies of Notices, Agenda, Notes on Agenda and other related papers of the transferor company, as handed over to the transferee company *[SS-1 – Clause 8.2]*	As long as they remain current or for eight financial years, whichever is later
17	Office copies of Notices, scrutiniser's report, and related papers of the transferor company, as handed over to the transferee company *[SS-2 – Clause 18.2]*	As long as they remain current or for eight financial years, whichever is later
18	Attendance register of general meeting *[Section 118 & Rule27 of Chapter VII]*	At least eight financial years
19	Register of Proxies [Section 105 & Rule 19 of Chapter VII]	At least eight financial years

SCHEDULE II

Business Area	Record	Disposal Policy
Corporate Governance	Records on establishment and development of the organization's legal framework and governance	8 years after the end of life of the organization
	Trustee Board papers and minutes	8 years after the end of life of the organization
	Management papers and minutes	8 years after the end of the financial year
	Subject Access Requests (requests and responses)	8 years from response
	Litigation with third parties	8 years after the settlement of a case
	Provision of legal advice	8 years from the date of advice
	Information Security Records	5 Years
	IT Records	3 Years
	Physical Security Records	1 Year
	Audit reports	8 years from completion
	Fraud Investigations	8 years from completion
	Customer Data	a. Maintenance of all necessary records of transactions between the RE and the customer, both domestic and international, for at least five years from the date of transaction. b. Preservation the records pertaining to the identification

		of the customers and their addresses obtained while opening the account and during the course of business relationship, for at least five years after the business relationship is ended. c. Call recording of customer's calls received a Call Centre for a period of 5 years. d. Electronic data of customer interactions for a period of 5 years
	Strategic plan, business plan, risk plans	8 years from completion
Data Protection	Consent (where unstructured data)	8 years after consent expired
	Privacy notices and index	8 years after the end of life of the organisation
	Record of Processing Activities	8 years after the end of life of the organisation
	Subject Access Requests	8 years after the end of life of the organisation
	Subject Access Request case data	90 days after the SAR case is closed
Financial Management	Financial records	8 years after the date of signing of accounts or, as applicable,
	Property acquisition (purchase, donation, rental, transfer) Deeds and certificates	8 years after the end of ownership/asset liability period
	Property leases	15 years after expiry
	General contracts and agreements	8 years after contract termination
	Unsuccessful tender documents	1 year after tender awarded
Human Resource Management	Job applications and interview records for unsuccessful applicants	6 months after the interview
	Payroll records – salaries and other payments through payroll	6 years
	Payroll records - Maternity, Paternity	3 years after the end of the tax year

	A summary of the record of service e.g. name, position, dates of employment, pay	6 years after the end of employment
	Timesheets, pay records and supporting documents such as contracts and contractual letters for employees charged to awards	5 years after payment of award balance
	All other HR documents	1 year after the end of employment