Shri Gajanan Lokseva Sahakari Bank Maryadit

Data Privacy Policy

1. Purpose

Objective The purpose of this policy is to maintain the privacy of and protect the personal information of employees, contractors, vendors, interns, associates, customers and business partners of Bank and ensure compliance with laws and regulations applicable (refer annexure A 'Data Privacy Annexures' document) to Bank.

2. Scope

This policy is applicable to all Bank employees, contractors, vendors, interns, associates, customers and business partners who may receive personal information, have access to personal information collected or processed, or who provide information to the organization. This Policy applies to all Bank employees, contractors, vendors, interns, associates, customers and business partners who receive personal information from Bank, who have access to personal information collected or processed by Bank, or who provide information to Bank, regardless of geographic location. all employees of Bank are expected to support the privacy policy and principles when they collect and / or handle personal information, or are involved in the process of maintaining or disposing of personal information. this policy provides the information to successfully meet the organization's commitment towards data privacy. All partner firms and any Third-Party working with or for Bank, and who have or may have access to personal information, will be expected to have read, understand and comply with this policy. No Third Party may access personal

information held by the organization without having first entered into a confidentiality agreement.

3. Definition

A privacy policy is a statement or legal document that discloses some or all of the ways a party gathers, uses, discloses, and manages a customer or client's data

4. Collection of Personal Information

Personal information may be collected online or offline. Regardless of the collection method, the same privacy protection shall apply to all personal information.

• Personal information shall not be collected unless either of the following is fulfilled:

- the data subject has provided a valid, informed and free consent;
- processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;
- processing is necessary for compliance with the organizations legal obligation;
- processing is necessary in order to protect the vital interests of the data subject; or
    - processing is necessary for the performance of a task carried out in the public interest

• Data subjects shall not be required to provide more personal information than is necessary for the provision of the product or service that data subject has requested or authorized. If any data not needed for providing a service or product is requested, such fields shall be clearly labelled as optional. Collection of personal information shall be avoided or limited when reasonably possible.

• Personal information shall be de-identified when the purposes of data collection can be achieved without personally identifiable information, at reasonable cost.

• When using vendors to collect personal information on the behalf of Bank, it shall ensure that the vendors comply with the privacy requirements of Bank as defined in this Policy.

• Bank shall at minimum, annually review and monitor the information collected, the consent obtained and the notice / SoW / contract agreement identifying the purpose.

• The project team/support function shall obtain approval from the IT Security team before adopting the new methods for collecting personal information electronically.

• Bank shall review the privacy policies and collection methods of Third-Parties before accepting personal information from Third-Party data sources.

• Personal information may only be used for the purposes identified in the notice / SoW / contract agreements and only if the data subject has given consent;

• Personal information shall be retained for as long as necessary for business purposes identified in the notice / SoW / contract agreements at the time of collection or subsequently authorized by the data subjects.

• When the use of personal information is no longer necessary for business purposes, a method shall be in place to ensure that the information is destroyed in a manner sufficient to prevent unauthorized access to that information or is de-identified in a manner sufficient to make the data non-personally identifiable.

• Bank shall have a documented process to communicate changes in retention periods of personal information required by the business to the data subjects who are authorized to request those changes.

• Personal information shall be erased if their storage violates any of the data protection rules or if knowledge of the data is no longer required by Bank or for the benefit of the data subject. Additionally, Bank has the right to retain the personnel information for legal and regulatory purpose and as per applicable data privacy laws.

• Bank shall perform an internal audit on an annual basis to ensure that personal information collected is used, retained and disposed-off in compliance with the organization's data privacy policy.

5. Disclosure to Third Parties

Data Subject shall be informed in the privacy notice / SoW / contract agreement, if personal information shall be disclosed to Third Parties / partner firms, and it shall be disclosed only for the purposes described in the privacy notice / SoW / contract agreements and for which the data subject has provided consent.

• Personal information of data subjects may be disclosed to the Third Parties / partner firms only for reasons consistent with the purposes identified in the notice / SoW / contract agreements or other purposes authorized by law.

• Bank shall notify the data subjects prior to disclosing personal information to Third Parties / partner firms for purposes not previously identified in the notice / SoW / contract agreements.

• Bank shall communicate the privacy practices, procedures and the requirements for data privacy and protection to the Third Parties / partner firms.

• The Third Parties shall sign a NDA (Non-Disclosure Agreement) with Bank before any personal information is disclosed to the Third Parties partner firms. The NDA shall include the terms on non-disclosure of customer information.

Security Information security policy and procedures shall be documented and implemented to ensure reasonable security for personal information collected, stored, used, transferred and disposed by Bank.

• Information asset labelling and handling guidelines shall include controls specific to the storage, retention and transfer of personal information.

• Management shall establish procedures that maintain the logical and physical security of personal information.

• Management shall establish procedures that ensure protection of personal information against accidental disclosure due to natural disasters and environmental hazards.

• Incident response protocols are established and maintained in order to deal with incidents concerning personal data or privacy practices.

6. Security and confidentiality of Customer Data

As per Information Systems security policies and procedures implemented in the Bank, Bank has implemented administrative, physical and technical safeguards to protect electronic personal data from loss, misuse and unauthorized access. Customers' personal data shall be stored on a secured database.

Bank shall not sell personal data to any third party or anybody and shall remain fully compliant with confidentiality of the data as per law.

Bank shall share customers' personal data to third party if required for business purpose only after implementing adequate controls to ensure maintenance of confidentiality and security of the data by the concerned third party.

Auto Read OTP functionality: -It is recommended that each process of OTP validation shall have auto read facility of OTP in the Mobile application. Whenever the OTP send to the customer, mobile app shall auto populate the OTP in the required field instead of entering by keypad.

SMS forwarding App / Remote access App: It is recommended that; the Mobile Application can have an ability to identify the "SMS forwarding Apps" as well as "Remote Access Apps" installed on the User's handset. Based on the "AppID" of these kind of Apps, Mobile App shall restrict the users to access the login to the application if user have installed the listed apps.

SMS Delivery status facility: SMS vendor should have Call back facility available to verify the status of SMS send from our end, also SMS vendor have "SMS Delivery receipt check" to know the delivery status of the SMS forwarded from our end.

Mobile banking Application shall have ability to read/detect Installed Application on user's device and upload it on bank's secure server for keeping safe track of existing applications. App shall prohibit/restrict Mobile Banking Application usage incase of any listed application with likes of remote access applications and sms forwarder applications is detected.

By agreeing to terms within Mobile banking application and written consent form undertaken from user during opting mobile banking feature it will be considered user have provided affirmative consent for all above mention disclosures.

7. Privacy Policy for SMS Autofill

This Privacy Policy describes how Mobile banking app collects, uses, and protects the information you provide when using the SMS autofill feature in our services.

8. Information We Collect:

Mobile banking app may collect and process the following information:

SMS Content: Mobile banking app may access and analyze the content of SMS messages to provide autofill suggestions for relevant information such as OTPs (One-Time Passwords) or transaction details.

Metadata: We may collect metadata associated with SMS messages, such as sender information, timestamps, and message status.

Usage Data: Mobile banking app may collect data related to your use of the SMS autofill feature,

How We Use Your Information:

Improving Autofill Accuracy: We use the information collected to improve the accuracy and relevance of autofill suggestions provided to you.

Security and Fraud Prevention: We use the information to enhance the security of SMS autofill and prevent fraudulent activities.

9. Sharing of Information:

Bank does not share your SMS autofill data with third parties except as described in this Privacy Policy or with your explicit consent.

10. Data Retention:

We retain SMS autofill data only for as long as necessary to fulfill the purposes outlined in this Privacy Policy or as required by law.

11. Roles and Responsibilities

The owner for the Privacy Policy shall be the Privacy Officer. the Privacy Officer shall be responsible for maintenance and accuracy of this policy. Any queries regarding the implementation of this Policy shall be directed to the privacy officer.

This policy shall be reviewed for updates by Privacy Officer on an annual basis. additionally, the privacy policy shall be updated in-line with any major changes within the organization's operating environment or on recommendations provided by internal/ external auditors.

12. Policy Compliance And Review

Compliance to the privacy policy shall be reviewed on an annual basis by Privacy Review Team to ensure continuous compliance monitoring through the implementation of

compliance measurements and periodic review processes. For proactive detection of data breaches, please refer breach management policy. In cases where non-compliance is identified, the privacy officer shall review the reasons for such non-compliance along with a plan for remediation and report them to Privacy Review Team.

Depending on the conclusions of the review, need for a revision to the policy may be identified. In instances of persistent non-compliance by the individuals concerned, they shall be subject to action in accordance with the Bank Disciplinary Policy.

Privacy Review Team shall conduct an internal audit annually (at minimum) to ensure compliance with the established privacy policies and applicable laws.

• The internal audit shall consist of the review of the following:

o personal information collected from data subjects;

o the purposes of the data collection and processing; o the actual uses of the data;

o disclosures made about the purposes of the collection and use of such data;

o the existence and scope of any data subject consents to such activities;

o any legal obligations regarding the collection and processing of such data, and

o the scope, sufficiency, and implementation status of security measures.

• The Privacy Review team shall document all the instances of non-compliance with privacy policies and procedures and report the same with the Privacy Management committee.

• The Data Privacy Officer along with Privacy Coordinators shall take actions on the findings from the internal audit and work on the recommendations for improvement of the privacy posture

• Any changes made to the policies shall be communicated to all the employees, the stakeholders and the customers / clients.

13. Amendments (Revision History)

Amendments to this policy will be published from time to time and circulated to the Bank.

Post-Implementation Policy Review: Annually

14. DOCUMENT HISTORY

As per version control sheet

*** End of Document **