



**SHIVA SAHAKARI BANK NIYAMITHA
DAVANGERE-577001**

**MOBILE BANKING PRIVACY
POLICY**

Document Control

Document Name	Mobile Banking Privacy Policy
Classification	Internal and Confidential
Document#	SHIVA SAHAKARI BANK NIYAMITHA DAVANGERE
Version	1.0
Date Released	01-MAY-2025

Document Ownership

Prepared By:	IT Department	Document Owner	IT Department
Approved By:	Board of Directors		

Copyright ©2025 Shiva Sahakari Bank Niyamitha Davangere. All Rights Reserved. This document contains sensitive & confidential information, and should not be disclosed to third parties without the prior written consent of Shiva Sahakari Bank Niyamitha Davangere. No part of this publication is reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of Shiva Sahakari Bank Niyamitha Davangere.

Sl No	Descriptions	Page NO
1	Introduction	3
2	Objective	3
3	Scope	3
4	Applicability	3
5	Coverage	3
6	Authority	3
7	Deviation	4
8	Violation	4
9	Handling of Misconduct	4
10	Review of the Mobile Banking Policy	4
11	Terminologies	4
12	Eligibility	5
	• Eligible Accounts	5
	• Ineligible Accounts	5
13	Services	5
14	Requirements to access Mobile Banking facility	6
15	Enrolment for the Mobile Banking Facility	6
16	Transaction Limit	6
17	Termination of The Mobile Banking facility	7
18	Roles and Responsibilities	7
19	Security FEATURES	8
20	Customer Grievance Redressal	9

1. Introduction

Shiva Sahakari Bank Niyamitha Davangere is a Urban Cooperative Bank, implemented the Core Banking Solution, surround applications and delivery channels from a common computing infrastructure. In the similar lines, common Mobile Banking policy is being evolved.

The Mobile banking service is a technology-based service that enables the bank to offer to its customers the banking services on the Mobile Handset. It facilitates the Mobile banking customer to get account information and transact with the bank electronically through Mobile handset.

Mobile Banking Policy sets out the guiding principles for Mobile Banking activities of the Bank. With respect to Information Security, the guidelines of IT Security Policy of the Bank are applicable to Mobile Banking Policy also. The guidelines issued by the Regulatory authorities' viz. RBI/Govt. of India on Mobile Banking services are applicable to this Mobile Banking Policy. The Guidelines are issued on these guiding principles to endure their compliance.

2. Objective

The objective of "Mobile Banking Policy" is to provide guidance and direction for the protection of the Bank's Mobile Banking facility provided to the customers as well as compliance of Mobile Banking Policy guidelines throughout the Bank.

3. Scope

The scope of Mobile Banking Policy is aimed to protect all the Mobile Banking services of the Bank against threats to their Confidentiality, Integrity and Availability

4. Applicability

- The Policy/guidelines/procedures contained herein shall apply to any person who has access to or who accesses Bank's Mobile Banking facility.
- This Policy/guidelines/ procedures shall be applicable to all the users at branches, service units and administrative units and the Mobile Banking customers unless otherwise specified in the document.
- The policy/guidelines/procedures shall be applicable to employees, customers, vendors, contractors, sub-contractors, external parties, Auditors and any other third party.

5. Coverage

- Mobile Banking policy includes all assets like people, process, data and information, software, hardware and communication networks etc. operated by the Bank, whether used locally or regionally or globally.
- These assets may be owned by the Bank, leased, hired, developed in-house or purchased.
- It includes services that are contracted or outsourced to other parties but operated for the Bank.

6. Authority

- The Mobile Banking Policy is issued under the authority of The Board of Directors of the Bank.

- The Mobile Banking Policy / Guidelines documents are confidential and strictly for internal circulation among the employees of the Bank Only.

7. Deviation

- Mobile Banking Policies / Guidelines / Procedures should be adhered to and any deviation shall be dealt with appropriately.
- The Staff and Contractual personnel should be aware of their responsibilities and operational requirements. Failure to abide by the provisions of Mobile Banking policy shall be dealt with suitably under the provisions of relevant Service Regulations, any other rule, settlements/agreements/instructions etc. issued by the Bank time to time.

8. Violation

- 1) No person of the bank or the contractors, vendors, and third parties shall violate the Mobile Banking Policy of the Bank.
- 2) The following acts on the part of personnel of the Bank or contractors, vendors, and third parties shall be construed as violation of Mobile Banking Policy.
 - a) Non-adherence to the standards / guidelines in relation to Mobile Banking policy issued by the Bank from time to time.
 - b) Any omission or commission which exposes the Bank to actual or potential monetary loss or otherwise reputation of Mobile Banking related systems and procedures.
 - c) Any unauthorized use or disclosure of Bank's confidential information or data.
 - d) Any usage of Bank's hardware, software, information or data for purposes other than for bank's normal business purposes and / or for any other illegal activities which may amount to violation of any law, regulation or reporting requirements of any law enforcement agency or government body.

9. Handling of Misconduct

- Failure to abide by the provisions of "MOBILE BANKING POLICY" by the personnel shall also be treated as misconduct under the relevant regulations applicable to them.
- Bank reserves the right to invoke the provisions of IT Act, 2000 and IT Amendment Act 2008 in addition to the above provisions.

10. Review of the Mobile Banking Policy

As Mobile Banking is undergoing rapid changes at a faster pace, Mobile Banking Policy needs to be reviewed by IT Security or as and when any major change in system usage or new system is introduced. Any feedback or suggestions for the improvement of these Guidelines may be referred to the IT Security for due consideration.

11. Terminologies

Account	Shall mean account at the bank which has been registered for Mobile banking facility
Customer	The holder of a bank account in Shiva Sahakari Bank Niyamitha Davangere
MPIN	Shall mean the Personal Identification Number (Password) for the Mobile banking Facility
SMS	Short messaging Service

Mobile Phone Number	Shall mean the Mobile number that has been registered by the customer for the Facility.
Application	Shall mean the Bank's Mobile Banking Application which will be downloaded on to the mobile Phone of the Customer
Bank	Shall mean Shiva Sahakari Bank Niyamitha Davangere or any successor or permitted assigns

12. Eligibility

Eligible Accounts:

The following types of accounts are eligible for the Mobile Banking facility.

- Savings Bank
 - Current Account
 - Overdraft
- a) Mode of operation for the accounts should be Individual/Self.
b) Existing Accounts should have satisfactory operations for reasonable period.
c) Account/s should be fully KYC compliant.
d) Newly opened accounts, depending upon the value of the account and at the discretion of the Branch in-charge.

Ineligible Accounts:

The following types of accounts are Ineligible for the Mobile Banking facility.

- Joint accounts
- Non-Resident Accounts
- Account/s of HUFs, Trusts, Clubs and Associations.
- Account/s under Court orders/Attachment orders.
- Inactive account/s.
- Corporate Accounts
- Frozen account/s for various reasons like disputes, litigation etc.
- KYC non-compliant accounts
- Minor Accounts.
- AOD Expired accounts
- NPA Accounts.
- Overdrawn / Limit expired Accounts

13. Services

The following facilities shall be provided under Mobile Banking Services

a) Account Information

- Account Overview
- Account History
- Account Details

b) Funds Transfer Interbank

- Same Bank Accounts
- Inter Bank Accounts

c) Customer Service

- Update Personal Info

- Cheque Orders / Stop Payments
- Online Account Opening
- Alerts
- d) Calculators**
 - Loan Calculator
 - Savings Calculator
- e) RDC Integration**
 - Mobile Remote Deposit Capture capabilities

14. Requirements to access Mobile Banking facility

Customers are required to have the following to access the facility.

Phase I:

- GPRS enabled Mobile Handset with WAP Browser /Mobile handset which supports JAVA/Android application
- Active Mobile Number

Phase II:

- Mobile Handset (any make)
- Active Mobile Number

15. Enrolment for the Mobile Banking Facility

The Customer desirous of availing Mobile Banking Application facility has to submit an application in the prescribed format in person, to the Branch Manager where customer is maintaining his/her account.

Accounts registered for Mobile Banking can be classified into two types:

- Primary Account
- Secondary Account

The primary account is the operative account indicated by the customer for receiving AADHAAR based credits (Through IMPS). In case the customer is having more than one operative account and wants to register all the accounts for mobile banking facility, he/she shall indicate one account as Primary and remaining as Secondary account/s.

However, customer can do transactions from all the registered accounts irrespective of whether the account is primary/secondary.

To start with facility of Mobile Banking is restricted to maximum of 2 accounts per customer. Once the customer is registered for Mobile Banking facility through menu-SMS REG and the same is verified, the Customer receives the MPIN, Application password on the end of the day of registration.

16. Transaction Limit

Bank shall impose the limits for carrying out funds transfer through various channels of Mobile Banking or any other services through Mobile Banking from time to time.

Periodically Bank will analyze market trend / customer requirements and bring in changes in fund transfer limit / transaction limit under various categories

17. Termination of The Mobile Banking facility

Mobile Banking facility for the customer should be withdrawn by Branches during the following instance:

- When the customer wants to close the Primary account registered for Mobile Banking
- When the customer wants to convert Primary account registered for Mobile Banking from Individual Self account to Joint account
- Resident Indian becoming Non-Resident
- Mobile Number is changed
- Change of customer id for Primary account registered for Mobile Banking
- Customer himself wants to deregister from Mobile Banking.

After terminating the customer in CBS, the branches should also immediately report the same to Administration Office through email for termination at Mobile Banking service. On receipt of such request, IT Wing shall terminate the customer from Mobile Banking as per branch request and confirm the same to Branches.

18. Roles and Responsibilities

BRANCH:

- a) Mobile banking will be issued only at the option of the customer/s, based on specific written or authenticated electronic requisition from the customer.
- b) On receipt of the request by the branch from the customer, Branch shall verify:
 - Whether all the columns are duly filled in.
 - Whether the signature of the customer appearing on the application with that of the specimen signature card tallies and whether certified to this effect by the Officer-in-charge
- c) It must be ensured that KYC guidelines are complied with by the customer, before extending the facility.
- d) Correctness of the address mentioned in the application vis-a-vis in the Finacle database shall be verified.
- e) Application form shall be preserved at the Branch itself.
- f) Branch will create the User-ID/s
- g) After login and MPIN change by the customer, activation has to be done by the Branch on request by the Customer.
- h) Register to be maintained for Branch Users and for User Profile of the customers.
- i) For any change in Mobile number/handset, written request from the customer has to be obtained, signature to be verified and to be authenticated by the Manager.

CUSTOMER:

- a) The customer will be responsible for all transactions, including fraudulent /erroneous transactions made through the use of his/ her SIM card/Mobile phone number and MPIN, regardless of whether such transactions are in fact entered into or authorized by him/ her. The customer will be responsible for the loss/damage, if any suffered.
- b) When Customer changes his Mobile Phone Number / is no longer using the Mobile Phone Number –customer shall take immediate action to deregister from Mobile Application.

- c) The Customer shall take all steps possible to ensure that his/her mobile phone is not shared with anyone and shall take immediate action to de-register from Mobile Application. As per procedure laid down in case of misuse/ theft/loss of the SIM card/Mobile Phone.
- d) The Customer will use offered facility using the MPIN in accordance with the procedure as laid down by the Bank from time to time.
- e) The Customer shall keep the Application password and MPIN confidential and will not disclose these to any other person or will not record them in a way that would compromise the security of the facility.
- f) It will be the responsibility of the Customer to notify the Bank immediately if he/ she suspects the misuse of the MPIN. He will also immediately initiate the necessary steps to change his MPIN.
- g) If the Mobile Phone Number or SIM is lost, the user must immediately take action to deregister from the facility.
- h) The Customer accepts that any valid transaction originating from the registered mobile phone number shall be assumed to have been initiated by the Customer and any transaction authorized by the MPIN is duly and legally authorized by the customer.

PROJECT MANAGEMENT OFFICE:

Hardware and software maintenance, vendor management, conveying our requirement to the concerned vendor, testing whether the product is working as per our requirement and implementation of services are the responsibilities of Project Management Office.

HEAD OFFICE:

Policy decisions, issuing of guidelines and Circulars, popularization of the Mobile Banking product, getting necessary permission from the Competent Authority/Committee for any modifications/amendments /additions/deletion in the existing Mobile Banking facility are the responsibilities of Development wing HO.

19.Security FEATURES

The following security features have been implemented in the Mobile Banking System.

- **Data Confidentiality:** Data and other information are kept highly confidential. This will not be disclosed to anybody unless legally warranted.
- **Encryption:** Data and messages travel in SSL 128bit end to end encryption while doing transactions on GPRS or WAP channel.
- **Change password Option:** Customers are provided with an option to change the MPIN at any number of times through application.
- **Password confidentiality:** MPINs are known to the respective customers only. The MPINs are randomly generated by the system and will not be known to any person in the bank.
- **Validity of Passwords:** There is no validity period for MPIN
- The Mobile Banking Solution will also have the security features as available for Core banking solution.

Two factor authentication is used for every financial and non-financial transactions:

- MPIN and Mobile Number are the two factors of authentication, when the transaction happens through Mobile Banking Application (GPRS).
- OTP (One time password), and MPIN are the two- factor authentication When the Transaction happens through WAP Channel
- Transactions, including inquiries are not permitted before changing default MPIN provided at the time of registration.

20. Customer Grievance Redressal

CHANNELS AVAILABLE FOR LODGING COMPLAINTS

- a) Bank's Website:** Complaints can be lodged online via the Online Grievance Portal available on the bank's corporate website www.shivasahakaribankdvg.com
- b) Physical Submissions at Branches or Offices:** Complaints may be submitted in writing through letters/forms or via email at any branch, office, or department of the bank, with an acknowledgment provided upon submission.
- c) Email:** Complaints/Feedback can also be sent to the following email addresses
 - customercare@shivasahakaribankdvg.com
- d) Contact Number: Landline No:08192-256107
Mobile No: 9449819322**
- e) Government & Regulatory Portals:** Customers can file complaints through government and regulatory portals such as RBI Ombudsman, CPGRAM (Centralized Public Grievance Redress and Monitoring System), INGRAM (Integrated Grievance Redress Mechanism)
