



Kerala Gramin Bank
Head Office: Malappuram

DIGITAL BANKING SERVICES WING

Mobile Banking Policy 2024-25

Table of Contents

1	Introduction	3
2	Objective	3
3	Scope	3
4	Applicability	3
5	Coverage	4
6	Authority	4
7	Deviation	4
8	Violation.....	4
9	Handling of Misconduct	5
10	Review of the Mobile Banking Policy	5
11	Terminologies	5
12	Eligibility	6
	12.1 Eligible Accounts:	6
	12.2 Ineligible Accounts:	6
13	Services.....	6
14	Requirements to access Mobile Banking facility	6
15	Enrolment for the Mobile Banking Facility	7
16	Transaction Limit	7
17	Termination of The Mobile Banking facility	7
18	Roles and Responsibilities	7
19	Security.....	8
20	Customer Grievance Redressal.....	9

1. Introduction

Pragathi Krishna Gramin Bank and Kerala Gramin Bank – Regional Rural Banks sponsored by Canara Bank – have come together for implementing 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.

Our RRBs are offering Mobile Banking facility in the name “PGBmPAY” for Pragathi Krishna Gramin Bank and “KGBmPAY” for Kerala Gramin Bank.

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

- a. The Policy/guidelines/procedures contained herein shall apply to any person who has access to or who accesses Bank's Mobile Banking facility.
- b. 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.
- c. The policy/guidelines/procedures shall be applicable to employees, customers, vendors, contractors, sub-contractors, external parties, Auditors and any other third party.

5. Coverage

- a) 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.
- b) These assets may be owned by the Bank, leased, hired, developed in-house or purchased.
- c) It includes services that are contracted or outsourced to other parties but operated for the Bank.

6. Authority

- a) The Mobile Banking Policy is issued under the authority of The Board of Directors of the Bank.
- b) The Mobile Banking Policy / Guidelines documents are confidential and strictly for internal circulation among the employees of the Bank Only. The discretion for making these documents available in full or in parts to any other party rests with Chief Information Security Officer/ PMO.

7. Deviation

- a) Mobile Banking Policies / Guidelines / Procedures should be adhered to and any deviation shall be dealt with appropriately.
- b) 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.
- c) For any deviation from Mobile Banking Policies or standards and guidelines in relation to the policies, PMO has to obtain approval from the competent authority/committee. Request for approval of deviation of Mobile Banking policy must provide the necessity for such amendment/addition/deletion.

8. Violation

- a) No person of the bank or the contractors, vendors, and third parties shall violate the Mobile Banking Policy of the Bank.
- b) 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.
 - i. Non-adherence to the standards / guidelines in relation to Mobile Banking policy issued by the Bank from time to time.
 - ii. Any omission or commission which exposes the Bank to actual or potential monetary loss or otherwise reputation of Mobile Banking related systems and procedures.
 - iii. Any unauthorized use or disclosure of Bank's confidential information or data.
 - iv. 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

9.2 Handling of Misconduct

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 DBS Wing annually 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/PMO 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 Kerala Gramin Bank
MPIN	Shall mean the Personal Identification Number (Password) for the Mobile banking Facility
KGBmPAY	shall mean Mobile banking facility offered by Kerala Gramin Bank
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 Kerala Gramin Bank or any successor or permitted assigns

12. Eligibility

12.1 Eligible Accounts:

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

- 1) Savings Bank
- 2) Current Account
- 3) Overdraft

- Mode of operation for the accounts should be Individual/Self.
- Account/s should be fully KYC compliant.

12.2 Ineligible Accounts:

1. Joint accounts
2. Account/s of HUFs, Trusts, Clubs and Associations.
3. Account/s under Court orders/Attachment orders.
4. Inactive account/s.
5. Corporate Accounts
6. Frozen account/s for various reasons like disputes, litigation etc.
7. KYC noncompliant accounts
8. Minor Accounts.
9. AOD Expired accounts
10. NPA Accounts.
11. Overdrawn / Limit expired Accounts.

13. Services

The following types of services are offered under the mobile banking facility.

- Balance Enquiry
- Mini Statement
- Funds Transfer Intra Bank (Within Kerala Gramin Bank)
- Funds Transfer Interbank (To other Bank through NEFT)
- Immediate Payment Services (IMPS)
- Stop Payment of Cheque
- Positive pay
- Inquiry facility on Cheque Status
- Hot listing/Limit setting of ATM Cards

14. Requirements to access Mobile Banking facility

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

- Mobile handset which supports JAVA/Android application (Android Version 6.0 and above) /IOS
- Active Mobile Number which registered with only one customer ID of Bank.
- Active ATM Card

15. Enrolment for the Mobile Banking Facility

The customer desirous of availing KGBmPAY facility has to download the application from google play store/apple store.

All eligible accounts of the customer is available and customer has to select the primary account.

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

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 stands terminated during the following instances:

1. When the customer closes all his eligible accounts.
2. Mobile Number is changed
3. Customer himself wants to terminate the application

18. Roles and Responsibilities

BRANCH:

1. For any change in Mobile number/handset, written request from the customer has to be obtained, signature to be verified and to be authenticated

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 KGBmPAY.
- 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 KGBmPAY 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. If the customer suspect the misuse of the MPIN, customer should immediately initiate necessary steps to change the 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

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 128 bit end to end encryption while doing transactions online.

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 generated by the customer himself/herself 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: Login PIN and Transaction PIN are the two factors of authentication, when the transaction happens through Mobile Banking Application

20. Customer Grievance Redressal

- a. For resetting the Login PIN/Transaction PIN, option for the same is provided in the application for the customer.
- b. Each Mobile Banking Transaction will have a unique Transaction ID which will enable us to track all types of transactions done through mobile banking.
- c. For any of their grievances, customers can approach their branch. The branches will direct the customers suitably and in case further assistance is required, branches can take up the matter with DBS Wing.
- d. Reporting tools/Reports are made available to track any transactions done through mobile banking.