Shri Gajanan Lokseva Sahakari Bank Maryadit

Mobile Banking Policy

1. INTRODUCTION

SHRI GAJANAN LOKSEVA SAHAKARI BANK MARYADIT. Founded in 1999 is serving for its customers on various channels. Being top bank in Co- Operative section, **SHRI GAJANAN LOKSEVA SAHAKARI BANK MARYADIT** Is providing its customers advance services and features. SHRI GAJANAN LOKSEVA SAHAKARI BANK MARYADIT has already launched its Internet Banking for customer and ready to move ahead on the next generation services of Mobile Banking.

In the age of electronic and mobile devices, banking sector has shown a tremendous growth. BANK has also taken various initiatives in order to keep in competition with growing banks. National Payment Corporation of India (NPCI) has developed Mobile Banking program for the Banks.

SHRI GAJANAN LOKSEVA SAHAKARI BANK MARYADIT has completed all necessary steps with NPCI and we have done the soft launch for IMPS i.e. funds transfer with mobile device person to person (P2P) and person to account (P2A) and Merchant payment. With merchant payment, module customers can pay the merchant via mobile device.

We are providing following services under mobile banking,

- Balance Enquiry
- Mini Statement
- IMPS-Funds transfer (Interbank & Intra Bank)
- Cheque book request

- Cheque status request
- Stop cheque request
- Email Statement request
- Physical statement request
- Account addition request
- ATM Pin re-generation Request

The application is developed in JAVA, Android. Blackberry phones and testing is in process for the same and expected to complete the development for other OS e.g. Apple Mobile banking application in this week. Apart from the above, we can incorporate the use cases for financial Inclusion in Mobile Banking Application.

The term **"Application Owner"** is referred to BANK Development Department and BANK Alternate Channels Department.

2. OBJECTIVE:

To achieve safe, sound and resilient mobile banking network and cash flow biding with the technological standards mentioned as per RBI and ITA 2000 and ITAA and other governing laws Intended Audience

The Policy is formulated for Bank and or the Banking cell taking in or working for the mobile banking related services

3. SCOPE:

The scope of the policy is to maintain the Confidentiality, integrity, authenticity and non-reputability while performing mobile banking transactions.

The bank shall provide following financial and non-financial services to its customers-

- Balance Enquiry
- Mini Statement
- Fund Transfer – through NEFT
- Immediate Payment System – To Mobile Number (P2P) and To Account Number (P2A)

- Cheque Book Request
- Cheque Status
- Stop Cheque
- Stop ATM card
- Locate nearby Branch / ATM
- View details of Deposits with the Bank
- Create Fixed Deposits / Recurring Deposits
- View details of Loan Accounts with the Bank
- Transfer funds to Loan Accounts
- Transfer funds from OD accounts to Savings / Current accounts and thereby withdraw cash using ATM cards, thus providing cash facility in case of an emergency.

4. DEFINITIONS:

In this document the following words and phrases shall have the meanings as set below unless the context indicates otherwise:

“Account(s)" shall mean any one or more accounts held and/or facilities provided to the Customer by Bank including but not limited to savings accounts, current accounts, term deposits or such other accounts and/or facilities as may be determined by Bank from time to time, for which the Facility is being offered or may be offered in future.

"Alert(s)" means the customized messages sent to the Mobile Phone Number as an SMS in response to the triggers set by the customer.

"Customer" shall mean a customer of BANK or any person who has applied for any product/service of BANK.

SHRI GAJANAN LOKSEVA SAHAKARI BANK MARYADIT.,.. is a primary Urban Co-op Bank registered as a co-op society in the year 1961. The register number of the bank is PNA/BNK/123/Year1999 dated 28/5/1999. The bank has been got banking license from the RBI in the year 1999. The license number is UBD.MUM.(MAH)0009 P/1999.2000 dated

25/10/1999. The area of operation of the banks is Pune district and bank is having 02 branches.

"MBS" shall mean Mobile Banking Service of the Bank and includes the service over the application/USSD/WAP/SMS Banking

"Mobile Banking" refers to the internet banking service offered or provided by bank to the User and which are described in the Terms by which the User may access information and give Name Bank instructions in respect of certain of User's Account(s) with the name Bank. Such Mobile Banking may be provided by bank directly or through its associates or contracted service providers or Affiliate.

"Mobile Banking app" shall mean the mobile banking application which can be installed on the mobile phone handset to access information pertaining to the Account(s).

"User" refers to a customer of bank and/or of the Affiliate of SHRI GAJANAN LOKSEVA SAHKARI BANK MARYADIT authorised to use Mobile Banking or a person requesting the Mobile Banking services.

"Personal Information" refers to the information provided by the User to Bank.

"SMS" shall mean Short Messaging Service, which is the transmission of short text messages to and from SMS enabled devices including but not limited to mobile phones.

"Service" or **"Facility"** shall mean mobile banking facility (which provides the Customers, services such as information relating to Account(s), details about transactions and such other services as may be provided on the Mobile Phone Number by BANK, from time to time.

Other abbreviations used:

RBI - Reserve Bank of India

NEFT - National Electronic Funds Transfer

RTGS - Real Time Gross Settlement

IMPS - Immediate Payment Service

MPIN - Mobile Banking Personal Identification Number

OTP - One Time Password

FD - Fixed Deposit

5. COMPLIANCE

Mobile Banking Service offered by **SHRI GAJANAN LOKSEVA SAHAKARI BANK MARYADIT.** would be in line with following, Mobile Banking guidelines Issued by RBI Regulations based on jurisdiction as may be modified from time to time Any governing provisions of other laws including Information Technology Act 2000, however, 2008 and amended 2011 ISO 27001 documents

6. SERVICE PROVIDED UNDER MOBILE BANKING

- The Bank shall implement this facility for almost all mobile platforms available in the market so that maximum number of customers can derive benefits out of this. Bank shall launch the Mobile banking applications for Android and iOS.
- The Bank shall offer services for transferring Funds within the Bank and even to accounts in other Banks. For this purpose, the Bank will join the Immediate Payment Services (IMPS) initiated by NPCI – both modes – Person to Person (Based on Mobile Number) and Person to Account (based on IFSC Code and Account Number).
  In addition to this, to offer more convenience the Bank shall enable customers to add beneficiaries once and then transfer the funds through NEFT channel, whenever required. However, there will be a cooling period of 24 hours as a security measure after addition of a beneficiary.

- Limits for fund transfer –

The Bank shall impose following limitations on Fund Transfer for transactions done using the application channel:

Sr No	Transaction channel	Per Day Per Account, Transaction Limit In Rupees.	Criteria
1	INTRA	2,00,000.00	Debit up to the available balance in account
2	NEFT	2,00,000.00	
3	IMPS (INTER)	2,00,000.00	

Accounts Type wise Eligibility for Mobile Banking :

Type of Account	Constitution	Mode of operation	Who is eligible for Mobile Banking facility
Saving Account (SB)	Single	Single	The account holder
	Joint	Either or Survivor	Allow to Main account holder only. However, application is to be signed by all account holders.
		Jointly	**Not Eligible**
Current	In the name of Individual	Single	The account holder

Account (CA)	In the name of Propritor	Single	The main account holder
		Jointly Operated	**Not Eligible**
Fixed deposit Account (Only View)	In the name of Individual	Single	The account holder
		Single /Joint / Either or Survivor	Main Account Holder.
		Jointly	**Not Eligible**
Loan/ CC/OD Accounts (Only View)	In the name of Individual	Any Type	Main Account Holder

Customers having following types of accounts will be eligible for Mobile Banking facility:

- **Fee Structure :**

Initially, the Bank shall not charge any fee for offering Mobile Banking Facility. However, the Bank reserves the right to charge the Customer fee for the use of the services provided under the Facility and change the fee structure at its discretion to comply RBI Guidelnes from time to time.

SHRI GAJANAN LOKSEVA SAHKARI BANK MARYADIT.,.. would provide following services to Mobile Banking users

Non — Financial

- Balance Enquiry
- Mini Statement (last 5transactions)
- Cheque Status
    a. Cheque Book request
    b. Stop Cheque request
    c. Cheque Status request
- Fixed Deposit Inquiry
- Change login / transaction passwords
- Manage Payee (registration of beneficiary)
- Demat balance inquiry
- Demat Statement (last 3transactions)
- Statement Request
    a. Email Statement request
    b. Physical Statement request
- Addition of Account request
- ATM PIN re-generation request

Financial

Funds Transfer (within Bank)

i) P2P (Person 2 Person) — funds transfer to mobile number
ii) P2A (Person 2 Account) — funds transfer to account number
iii) P2M (Person 2 Merchant) — Merchant payments
iv) Self-Linked Accounts
v) Third Party Transfer
vi) Utility Bill Payment,
vii) Stop Payment of Cheques,
viii) Railway reservation

Immediate Payment Service (IMPS)

i) Through MMID (Mobile Money Identifier — P2P)
ii) Through IFSC (Account Number — P2A)
iii) Generate / Retrieve / Cancel MMID
iv) Manage Beneficiary

Bank to offer Mobile Banking facility to the customer subject to a daily cap of Saving Customer is Rs.1, 00,000/- & Current Account Holders is Rs. 2,00,000/- per customer for both fund transfer and transaction involving purchase of goods.

7. MOBILE BANKING ROLES AND RESPONSIBILITIES

Operations Team: This team is responsible for managing technical changes with respective of customer, Reconciliation, Dispute Management

Admin Team: This team is responsible of admin operations such as Registration, MPIN generation, Account addition; generate reports, print transaction password, NPCI Coordination etc.

Internal User

Mobile Banking back office is handled centrally at HO by Mobile Banking Admin staff. There would be separate user IDs created for each user. A grand user named Super Admin shall have access to create and delete/suspend admin users.

Admins are divided into two groups as Maker Admin and Checker Admin. Maker Admin shall enter any request of enter data into the portal and Checker Admin shall verify everything entered by Maker Admin.

Registration

Mobile Banking Service is given to the customers under following schemes,

Account Type	Account Operation	Scheme Type
SB	Self	All SB Schemes except minor
	Either or Survivor (First holder)	
	Either or Survivor (First holder)	
	Any one (First Holder)	
CA	Proprietor	All CA Schemes

Mobile registration for additional accounts will be done for those accounts, which are having account type as defined in above table and which are listed under same customer ID.

Password

Each user of Mobile Banking application will be allotted three types of passwords,

- **MPIN:** This is a 4 -digit password used in order to log into the Mobile Banking Application and used under some requests such as generate OTP etc.
- **Transaction Password:** This is an alpha numeric password with 6-8 characters used for funds transfer (Inter Bank & Intra Bank)
- **OTP:** This is a 6- digit one-time password (one hour expiry) used for SMS based transactions as well for making merchant payments
- **MMID:** This is not a password but a 7-digit number assigned to an account in order to receive funds from other parties.

Transaction Password printing

After successful registration, a hard copy of transaction password is generated for each user. Transaction Password will be printed by a user who authorizes records
This password is then be stuffed into envelops and sent to respective branch through internal Currier.

Funds transfer

With Mobile Banking application users can send i.e. remit funds from their account to either another mobile i.e. P2P (Person 2 Person) or another account i.e. P2A (Person to Account). Users can remit funds either by Mobile Banking application (JAVA, Android, iOS, Windows)

or by WAP (Wireless access Protocol) i.e. with the use of Internet connection on mobile or by SMS. Each of these types are associated with limits as follows,

For Application and WAP: Daily limit is INR 50,000 and calendar month limit is INR 2,50,000

For SMS based: Daily limit is INR 1,000 and calendar month limit is INR 5,000

Beneficiary Limit-NO LIMIT

Service Cancellation

The customer may request for cancellation of the Mobile Banking account any time by giving a written notice to home branch. The cancellation shall take effect on the completion of the process at Mobile Banking Cell.

The customer will remain responsible for any transactions made through Mobile Banking until the time of such termination.

SHRI GAJANAN LOKSEVA SAHKARI BANK MARYADIT.,.. will suspend the Mobile Banking account access anytime either entirely or with reference to a specific service or customer in following cases

In case of breach of Terms by the customer.

If it learns of the death, bankruptcy or lack of legal capacity of the customer, then the main account at the branch is closed which automatically closes the Mobile Banking account through legal advice.

Service will also get cancelled or suspended if user deletes/cancels all the MMID associated with mobile number (this is an online request can be given using Mobile Banking application or SMS)

Cheque book request

Customers can give chequebook request via Mobile Banking Application/SMS. Only one chequebook request is accepted in a month.
Chequebook requests are to be given to Admin department for further processing with 10/20 pages personalized chequebook for saving account and 50 pages personalized cheque book for Current account.

Chequebook charges are debited to customer account as required and as per the current Bank policy

MB cell shall demand chequebook inventory from Admin department as required

Cheque Book Return

If chequebooks are not delivered to customers and if returned then Admin department should contact customer for resending the chequebook

Admin department will call customer/branch and ask customer to collect the same from admin department

After 90 days, chequebook will be destroyed.

Account addition

The mobile banking users can add accounts having account similar to registered account. For e. g. saving and current having operation as per registration policy, By using account addition request user can add multiple accounts listed under users customer id registered for Mobile Banking.

The following should be enforced for customer accounts:

- The application should enforce minimum password length of 6 characters and maximum length of 8.
- System should not display the password as it is keyed in.
- Passwords should be alpha numeric combination.
- Application should enforce account lockout. Account lockout configured for 3 failed login attempts.
- Application should force new customer to change the password at first login as well as every fresh login.

Charges for request

For Mobile Banking Requests bank should recover charges from customers in following cases There are no additional charges apply to customers for availing Mobile Banking facility for 1st year. All the charges for physical statement, stop cheque, ATM pin re-generation will apply as per the current branch policy.

Data Security

Adequate controls should be implemented to ensure confidentiality and integrity of data. 128-bit SSL should be enabled on the Mobile Banking Server to encrypt customer login and transaction details. Following types of areas must be monitored daily,

- Unauthorized user accessing information
- Loss of Data integrity
- Transaction flow

Security testing

Application should be tested for compliance with security policy before deployment. This includes following areas,

- Testing needs to be done whenever there is a major application change including version upgrade
- All vulnerabilities should be discovered and identified during the testing and fixed before application is deployed in production environment.
- Mobile Banking structure is subjected to periodic Black Box penetration testing and Vulnerability Assessment

Audit Logs

A tracking in the Mobile Banking portal for each user is to be in place to capture latest changes done by users. If any users perform any action, i.e. generate MPIN or modify customer data then those users' details are captured for the audit purpose.

Customer Account Security

All new Mobile Banking customer accounts shall be created only after offline verification of credentials. Customer should not have the provision to create new account on mobile.

No one including the Bank employees should have access to the customer's Mobile Banking password while it is being generated and distributed.

Transaction password should be securely dispatched to the customer on a separate PIN mailer.

Customer should be informed about security measures to be adhered for secure Mobile Banking in the following areas

- MPIN
- Transaction password

These guidelines should be communicated to the customers either along with the password or by publishing user manual guide for customer or by publishing on the Mobile Banking web site (https://www.gajananbank.com/pricacyPolicy). Application owner is responsible for updating these guidelines based on new threats.

Server Security

The Mobile Banking application services should be protected by a firewall. Based on the risk levels the servers and external connections should be segregated across multiple segments.

The firewall can have the following segments:

i) Web Server
ii) Application Server
iii) Database Server

The system admin team in consultation with the product head should design the firewall segments and rule base.
The firewall should limit access to essential IP-Address/Ports.
There should be no direct dial up access to any of the Mobile Banking service. If dial up access needs to be provided, the dial up server should be separated from the mobile banking servers by a fire wall.

Redundancy

Adequate redundancy should be built into the network links

Anti-virus

Anti-virus software should be installed on all machines with risk of virus infection.

Backup

Backup process

Backups should be taken regularly to ensure that the data could be recovered when required as per the Information Security Policy of the Bank.

The application owner should identify the essential components that need to be backed up including the following:

- OS and application files
- Configuration files
- Data files
- Logs
- Web server logs
- Oracle Database server logs

Backup scheduling

Backup should be scheduled during non-peak usage hours.
Backup should take before and soon after any change in the application environment including application hardware upgrade.
The application owner should take into account the following parameters when deciding the type of backup, frequency of the backup and the type of media:

- Volume of transaction

- Criticality of data
- Recovery time constraints

Retention period is required for determining the rotation cycle for back up media and also for deciding on erasing old data for creating free disk space. This retention period is defined as per the standard Policy document of BANK

Security of Data on the Backup Media

Back up should protect as per the information security policy of the Bank. Attention is invited in particulars to the following areas:

- Prevention of unauthorized access to backup media
- Offsite storage and maintenance of appropriate environmental conditions
- Secure disposal of backup media
- Recovery testing of backup media

Migration of Backup Data

If there is a change in business application software or application used for taking backup, all previously backed up data that needs to be retained should be migrated to a format that is readable by the new application. If there is a change in backup media. all previously backed up data that needs to be retained should be transferred to the new media.

Monitoring

- **Log monitoring**

- Date and time on all Core Banking Servers at Data Center should be set correctly to Indian Standard Time.
- OS database and application logs of the servers at Data Center should be monitored on daily basis.
- Automated tools should be used for analyzing the logs. System Admin team should identify and document all events that need to be tracked in the logs. The logs should be analyzed for events that would affect the security of the system including the following:

    1) Account created/deleted/disabled
    2) Password change for privileged account
    3) Start and stop of service
    4) Authentication failures
    5) System error or failures

- Change in configuration settings including file permissions or user privileges Application owner should nominate a team responsible for analyzing the log

files and taking actions. Application owner should ensure that the same person whose activities are getting logged does not do log analysis. There should be separation of duties to ensure the independence.
The security team should generate log report quarterly detailing security incidents observed in the logs and the action taken. This report should submit to the product head.

- **Security Monitoring**

Network based IDS should be setup to monitor all access to Mobile Banking Service. Application owner should nominate a team responsible for analyzing and reporting on attacks detected by IDS.

The team responsible for IDS monitoring should generate weekly report on attacks detected and action taken. This report should be submitted to the application owner.

8. PHYSICAL SECURITY

Centralized IT assets of Mobile Banking should be hosted in Data Center. Data center should have Physical protection as per the Information Security Policy of the Bank.

The Bank has assured that sensitive customer data, and security and integrity of transactions are protected. And also taking necessary steps/actions for the mobile banking servers at the bank's end or at the mobile banking service provider's etc. and the Bank has followed ISO Standards and implementing as per Information Technology Act.

Application Owner should implement adequate physical security of IT assets related to Mobile Banking located outside the Data Center as per the physical security policy of the Bank.
The physical security measures should include-

- ✓ Physical access control with Identification and Authorization checks
- ✓ Redundancy in the power supply
- ✓ Environmental protection against temperature. fire, humidity, water, dust
- ✓ External recognized penetration testers in accordance with Security policy should test all security infrastructures periodically.
- ✓ In addition, banks should conduct regular information security audits on the mobile banking systems to ensure complete security.

9. INCIDENT MANAGEMENT

An incident is a violation of an explicit or implied security policy.
The following actions can be classified as incidents:

- Abnormal system resource usage-If the Mobile memory utilization on a system is very high, the system could have been compromised. Attackers used compromised system for spreading viruses or attacking other Mobile leading to high resource utilization system administrators need to track resource utilization and analyze reason for any abnormal usage.
- Users experience slow response- End user could experience slow response times if the application servers or the network has been compromised and is being used for malicious purpose. Virus or worm outbreak could lead to network congestion that would in turn cause application response to be slow and unstable. End users should report any drastic drop application response or system stability to system administrators.

- Data Corruption- Unauthorized modification or deletion of data or in ability to retrieve data incorrect format, web defacement

- Changes in user passwords — user should report to system administrator if they are not able to access the application with their passwords any authorized changes in user passwords: addition/ deletion of user accounts could be indication of system compromise.

- Traffic on non-essential ports - if there is network traffic on ports that are not used by any of the internal application this could be sign of a back door application in the network. The traffic should be tracked and reported by a monitoring team. If the backdoor application tries to traverse the firewall. the fire wall logs would track these.

- Attempts to gain unauthorized access — successful/unsuccessful attempts to gain access to the IT system and application supporting the Mobile Banking Application

- Unwanted disruption or denial of service — changes to the system hardware, firmware software characteristics without the application owner' s knowledge

- All internal users and system administrators of Mobile Banking should be responsible for identifying and reporting incidents. The system administrator should do a preliminary analysis to ascertain the cause and extent of damage.

- An incident report should be sent to the appropriate authorities in the Bank in the format laid down by the Bank's information Security Policy.

The bank may acquire necessary tools and systems for attacks.
The overall Information System Security Policy as applicable would govern the selection of the tools and systems. The policy will be reviewed by the application owner every year or at the time of any major changes in the existing environment, which would affect the areas, covered in this policy.

Reporting

The Mobile Banking System or The Mobile Banking Department should generate sufficient reporting to satisfy daily monitoring and control of transactions and activities. Additionally appropriate reports should be generated that provide the necessary information to track the effectiveness of the program. The Mobile Banking coordinator will report Mobile Banking activities to the executive committee on a quarterly or as needed basis.

Internal Audit and compliance

The internal Auditor and compliance officer will conduct a review of Mobile Banking on a quarterly basis. A report will be rendered to the Audit Committee.

Internal Audit and compliance

All financial product and services contain an element of risk, making effective risk management essential. Risk management is comprised of several factors:

- Θ Identifying the risk
- Θ Understanding the implication of the risk
- Θ Measurement of the risk
- Θ Setting acceptable risk tolerances and parameters
- Θ Maintaining risk at acceptable levels

10. TECHNOLOGY AND SECURITY STANDARDS

Fundamental of payment systems

SHRI GAJANAN LOKSEVA SAHKARI BANK MARYADIT.,.. is implementing Technology standards and security controls as per the RBI guidelines circular DPSS. CO. PD. Mobile Banking. Bo.2/02.23.001/2014-15 dated July 1. 2015. However. The bank is complying IT Framework, technology deployed is fundamental to satisfy and soundness of Mobile Banking payment system. Therefore. BANK is complying and following the Security Standards appropriate to the complexity of service offered, subject to following minimum standards set out as per the Mobile Banking Policy. As per the RBI Guidelines, the Bank has applied in a way that is appropriate to the risk associated with services provided by the Bank and the system which supports these services.

Transaction Limits

SHRI GAJANAN LOKSEVA SAHKARI BANK MARYADIT.,.. is offering mobile banking facilities (financial) to its customers. Interbank Mobile Payment Service (IMPS) developed and operated by National Payment Corporation of India (NPCI) has also enabled real time transfer of funds through the medium of the mobile phone between accounts in different banks. The volume and value of mobile banking transactions is also showing in uptrend.

In terms of Para 2.1 of RBI circular dated December 24, 2009, a transaction limit of Rs. 50,000/- per customer per day had been mandated. On a review, it has been decided to remove this cap. However, BANK, should place per transaction limits based on their own risk perception with the approval of its Board.

It is also clarified that the directions under Para 2 "Remittance of funds for disbursement in cash" of RBI circular dated December 24, 2009 stands superseded with the directions contained in its circular RBI/ 2011-12/213 DPSS. PD. CO. No. 622/02.27.019/2011-2012 dated October 05, 2011. Banks are required to put in place appropriate risk mitigation measures like transaction limit (per transaction, daily, and weekly, monthly), transaction velocity limit, fraud checks, AML checks etc. depending on the bank's own risk perception, unless otherwise mandated by the Reserve Bank.

AML checks

SHRI GAJANAN LOKSEVA SAHKARI BANK MARYADIT.,.. is operating customers' accounts as per the Anti Money Laundering Act / KYC Guidelines. As per the RBI Guidelines, BANK, offering money transfer facility subject to adherence of KYC/AML Guidelines. BANK, is providing Money Transfer facility in safe, secure and efficient manner breadth of country. For this facility, the following terms are necessary.

Enabling transfer of funds among domestic debit/credit/pre-paid cards subject to the same transaction/monthly cap as at (ii) above.

Authentication

SHRI GAJANAN LOKSEVA SAHKARI BANK MARYADIT.,... is providing mobile banking services to its customers and also complying with the following security principles and practices for the authentication of mobile banking transactions:
All mobile banking are permitted only by validation through a two factor authentication.
One of the factors of authentication is MPIN or any higher standard.
When MPIN is used, end-to-end encryption of the MPIN shall not be in clear text anywhere in the network.
The MPIN shall be stored in a secure environment.

Level of Encryption and security standards

SHRI GAJANAN LOKSEVA SAHKARI BANK MARYADIT.,... is having Proper level of encryption and security and implementing at all stages of the transaction processing. The end ever are taken to ensure end-to-end encryption of the mobile banking transaction. Adequate safe guards are also in place to guard against the use of mobile banking in money laundering. Frauds, etc. As per guidelines laid down in RBI circular with respect to network and system security are followed:

Implementing application level encryption over network and transport layer encryption wherever possible.

Establishing proper firewalls, intruder detection system (IDS), data file and system integrity checking, surveillance and incident response procedures and containment procedures. Conducting periodic risk management analysis, security vulnerability assessment of the application etc. at least once in a year.

Maintaining proper and full documentation of security practices, guidelines, methods, and procedures used in mobile banking and payment systems and keep them up to date based on the periodic risk management, analysis and vulnerability assessment carried out.

Implementing appropriate physical security measures to protect the system gateways, network, equipment, servers, host computers, and other hardware/software used from unauthorized access and tempering. The Data Centre of the Bank and Service Providers should have proper wired and wireless data network protection mechanisms.

11. PHYSICAL SECURITY MEASURES

The dependence of banks on mobile banking service providers may place knowledge of bank systems and customers in a public domain, Mobile-banking system may make the banks dependent on small firms (ie. mobile banking service providers) with high employee turnover. It is therefore, imperative that sensitive customer data, and security and integrity of transactions are protected. It is necessary that the mobile banking servers at the bank's end or at the mobile banking service provider's etc. if any, should be certified by an accredited external agency. In addition, banks should conduct regular information security audits on the mobile banking systems to ensure complete security.

12. INFORMATION SECURITY AUDITS ON MOBILE BANKING SYSTEMS

For channels which do not contain the phone number as identity, a separate login ID and password are provided to ensure proper authentication, Internet Banking login ID's and Passwords are not be allowed to be used for mobile banking.

The Bank is complying as per the Reasonable Security Practices & Procedures as per the Sec. 43A of IT Act, 2011 and also implementing technology standards as per RBI Guidelines of its circular issued in 2014-15 for the sake of Information Security breach, Bank is conducting regular Information Security Audits on Mobile Banking Systems to ensure safe, secured and soundness payment system to its customers. The Bank is conducting VNPT reports on yearly basis in this respect for audit purpose.

Customer Protection Issues

Security procedure

The security procedure adopted by the BANK for authenticating users is recognized by law as a substitute for signature. As per RBI guidelines and information Technology Act. 2000. 2008 and amended 2011. The bank is providing particular technology and security procedure as a means of authenticating electronic record.

Authentication on Legal Risk

All the terms and conditions related to authentication procedure and legal risks of the customers are displayed as per RBI norms on our website. Bank shall ensure to its customers that they are made aware of the said legal risk prior to sign up.

Risk Control Measures

SHRI GAJANAN LOKSEVA SAHKARI BANK MARYADIT.,... is maintaining secrecy and confidentiality of customers' accounts. In the mobile banking scenario, the risk of bank not meeting the above obligation is high. The BANK is exposing enhanced risk of liability to customers on account breach of secrecy. denial of service. etc. on account of hacking/other technological failures. Therefore, the Bank is, instituting adequate risk control measures to manage such risks.

As per RBI guidelines BANK is disclosing risks, responsibilities and liabilities of the customers on their websites and/or through printed material.

No Stop Payment Privilege

As in an Internet banking scenario, in the mobile banking scenario too, there is very limited or no stop-payment privilege for mobile banking transactions since it becomes impossible for the banks to stop payment in spite of receipt of stop payment instruction as the transactions are completely instantaneous and are incapable of being reversed. Hence BANK offering mobile banking should be notified by the customers the time frame and the circumstances in which any stop-payment instructions could be accepted.

Precautionary Measures as per Consumer Protection Act.

The Consumer Protection Act, 1986 defines the rights of consumers in India and is applicable to banking services as well. Currently, the rights and liabilities of customers availing of mobile banking services are being determined by bilateral agreements between the banks and customers. Taking into account the risks arising out of unauthorized transfer through hacking, denial of service on account of technological failure etc. banks providing mobile banking would need to assess the liabilities arising out of such events and take appropriate counter measures like insuring themselves against such risks, as in the case with internet banking.

Payees and Payee's banks rights and obligations

Bilateral contracts drawn up between the payees and payee's bank, the participating banks and service provider should clearly define the rights and obligations of each party.

Terms and conditions on websites

The existing mechanism for handling customer complaint/s grievances may be used for mobile banking transactions as well. However, in view of the fact that the technology is relatively/new, BANK has set up a help desk and disclosed the details of the help desk and escalation procedure for lodging the complaints, on our website. A detail regarding the above procedure is made available to the customer at the time of sign up.

Responsibility and liabilities of customer

In cases where the customer files a complaint with the bank disputing a transaction, it would be the responsibility of the service providing bank to expeditiously redress the complaint. Banks may put in place procedures for addressing such customer grievances. The grievance handling procedure including the compensation policy should be disclosed.

Customer Complaint Grievances

Customers' complaints/grievances arising out of mobile banking facility would be covered under the Banking Ombudsman Scheme 2006 (as amended up to May, 2007).

Customer complaints covered under Banking Ombudsman Scheme 2006
The jurisdiction of legal settlement would be within India.

13. PERCEIVED RISKS AND MITIGATION MEASURES:

The perceived risks under Mobile SMS Banking and mitigation measures are given hereunder:

Sr. No.	Risk Factor	Risk Mitigation
	Technology and Security Standards	
1	Banks are required to put in place transaction limit (per transaction, daily, weekly, monthly) transaction velocity limit, fraud, checks, AML checks etc. depending on the bank's own risk perception by the Reserve Bank.	Configuration in Mobile B5anking application enables Bank to put in place measures such as Transaction 1imits, Velocity limit etc. & the same will be put- in place as per outer limits prescribed by RBL As regard fraud checks. the initiation of the mobile Banking transaction is validated using the combination of

		mobile number and Mobile Handset identity number (IMEI) Mobile Handset identify number is captured by the mobile Banking application, when the customer activates the application by using the secured pin (M-PIN that is known only to the customer as the PIN mailer containing the secured PIN is given to the customer after physical identification at the branch by official concerned
2	Authentication of the Mobile Banking Transactions	All Mobile Banking transactions will be permitted by validation using multi factor Authentication method that is a combination of Mobile number Mobile Handset identity number and also M-PIN and login password which will be set by the customer at the time of activation of mobile Banking application
3	Protection of the data	End-to-end protection of data will be done, as the data will be encrypted using internationally recognized SSL encryption standards. SSL encryption communication is established between the mobile handset and mobile server
4	System and Network Security	The Mobile Banking application and database is hosted in highly secure Data Centre (DC) of the Bank Network security and access controls at DC Comply with the laid down Guidelines Price water house has done the audit of the network and security at Data Centre. Audit of the network for the current year is in progress.

5	Protection of the customer data	Mobile Banking application will be hosted in Bank's own domain so that entire application and data is in its control. Bank would further ensure that Mobile Banking application hosted at Bank's Site is certified by an accredited external agency and also vulnerability assessment of the application is done every year
Customer protection issue		
6	Secrecy and Confidentiality customer accounts	The registration for the service will be document based and physical presence of the customer at the Branch and authentication of his identity will be Mandatory.
7	Customer complaints and grievances	A helpdesk for Internet Banking Is operational 247. The strength of the help desk team would be suitably increased and they would also be trained to enable them to manage the Help Desk or Mobile Baking also
Disclosures of risks and liabilities		
8	Disclosures of risks, responsibilities and liabilities of the customers on their websites and/or through printed material.	The terms and conditions applicable for availment of the Mobile Banking facility as finalised by Legal and risk Management Department(s) will be printed as a part of Application tor registration. The same would also be published on Bank's website before launch of the facility. The copy of terms and conditions is enclosed.

The above perceived risk and mitigation thereof have been vetted by IRM Department.

14. REVIEW OF POLICY

Chairman & Mg Director, or in his absence, Executive Director shall be the competent authority to revise or amend or modify or annul any or all of the

provisions contained in this policy at any time or from time to time based on the recommendations of the General Manager(IT)

In emergent situations, subject to ratification by the Chairman & Mg Director, or in his absence, Executive Director, General Manager (IT) will be the competent authority to effect necessary changes in this Policy.

The policy and operating guidelines governing the Mobile Banking Policy & Services of the Bank shall be reviewed annually.

15. REFERENCES:

This policy has been drafted with reference to the guidelines issued by the Reserve Bank of India on Mobile Banking Policy.

a. DPSS.CO.No.619 /02.23.02/2008-09 - Mobile Banking Transactions in India - Operative Guidelines for Banks dated 08.10.2008
b. DPSS.CO.No.1357/02.23.02/2009-10 - Mobile Banking Transactions in India - Operative Guidelines for Banks dated 24.12.2009
c. DPSS.CO.No.2502/02.23.02/2010-11 - Mobile Banking Transactions in India – Operative Guidelines for Banks dated 04.05.2011
d. DPSS.PD.CO.No.622 /02.27.019/2011-2012 - Domestic Money Transfer- Relaxations dated 05.10.2011
e. DPSS.CO.PD.No.1098/02.23.02/2011-12 - Mobile Banking Transactions in India – Operative Guidelines for Banks dated 22.12.2011
f. DPSS. CO. PD. No. 1098 / 02.23.02 / 2011-12 - Mobile Banking Transactions in India – Operative Guidelines for Banks dated 04.12.2014

16. CUSTOMER COMMUNICATION

Customers can communicate with Bank's Customer Care for Mobile Banking related matters 24x7 through below mentioned channels:

Contact number: 020 27371290

Email:- ho@gajananbank.com

Letters and couriers may be addressed to: GP-187/3, G - Block, MIDC, Thermax Chowk, Sambhajinagar, Chinchwad, Pune – 411019

Roles and Responsibilities

The Administrative Management is responsible for approval and execution of the Policy. The policy shall review on yearly basis.

17. 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.

18. 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.

19. 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.

20. 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.

21. 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.

22. INQUIRIES

Inquiries regarding this policy can be directed to the Head of Information Security/CEO.

23. AMENDMENTS (REVISION HISTORY)

Amendments to this policy will be published from time to time and circulated to **SHRI GAJANAN LOKSEVA SAHKARI BANK MARYADIT.,...**

Post-Implementation Policy Review: Annually

24. DOCUMENT HISTORY

As per version control sheet

*** End of Document ***