1 INTRODUCTION

Pune Urban Co Op Bank Ltd sponsored by HDFC Bank have come together for implementing 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 APLICABILITY

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.

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, CISO 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 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 Act2008 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/CISO 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/CISO 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 Pune Urban Co Op Bank Ltd
MPIN	Shall mean the Personal Identification Number (Password) for the Mobile banking Facility
GRPS	General Packet Radio Service
SMS	Short Messaging Service
WAP	Wireless Application Protocol
USSD	Unstructured Supplementary Service Data
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 Pune Urban Co Op Bank Ltd or any successor or permitted assigns

12 ELIGIBILITY

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

a. Savings Bank

b. Current Account

Mode of operation for the accounts should be Individual/Self.

Existing Accounts should have satisfactory operations for reasonable period.

Account/s should be fully KYC compliant.

Newly opened accounts, depending upon the value of the account and at the discretion of the Branch in-charge

13 SERVICES

a. Balance Enquiry
b. Mini Statement
c. Funds Transfer Intra Bank
d. Funds Transfer Interbank
e. Immediate Payment Services (IMPS)

14 Requirement to Access Mobile Banking Facility

a. Customers are required to have the following to access the facility.
b. GPRS enabled Mobile Handset with WAP Browser/Mobile handset which supports Android application
c. Active Mobile Number
d. Mobile Handset (any make)

15 Enrolment for the Mobile Banking Facility

The Customer desirous of availing Mobile Banking 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 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 the Mobile Banking facility customer has to download the application from the Google Play Store and install the same in the mobile handset where the registered mobile number SIM card is available and is active. For the first time use the customer has to generate the MPIN of his choice which is 4 digits in length. The MPIN generation is secured way having combination of some of customer details and the OTP. After the successful generation of the MPIN customer can use the Mobile Banking Facility provided by the bank.

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:

- **a.** When the customer wants to close the Primary account registered for Mobile Banking
- **b.** When the customer wants to convert Primary account registered for Mobile Banking from Individual Self account to Joint account
- **c.** Resident Indian becoming Non Resident

d. Mobile Number is changed
e. Change of customer id for Primary account registered for Mobile Banking
f. Customer himself wants to deregister from Mobile Banking.

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:

i. Whether all the columns are duly filled in.

ii. 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 compiled by the customer, before extending the facility.

d. Correctness of the address mentioned in the application vis-à-vis in the database shall be verified.

e. Application form shall be preserved at the Branch itself.

f. 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 Banking Facility.

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 Banking Facility 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 suspect 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.

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 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 generated by the system 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 authentications are used for the using Mobile Banking Facility. MPIN and Mobile Number are the two factors of authentication and when the transaction happens through Mobile Banking the OTP is generated and send to registered mobile number as a third factor authentication for financial transaction.

20 Review of the Policy

This policy will be reviewed annually keeping in view the guidelines / directions issued by RBI, Ministry of Finance, Board of Directors and Audit observations etc.

For PUNE URBAN CO OP BANK LTD. LTD.