The District Co-operative Central Bank Ltd., Mahabubnagar

Mobile Banking Policy

IT Department

Head Office, Telangana Chourastha, Mahabubnagar – 509 001

DOCUMENT CONTROL

Document Title: Mobile Banking Policy

Document ID : DCCB-IT-MBP-01

Version : Version 1.0

Document Owner: IT Department

Revision History:

S. No.	Author Name	Version Number	Date	Remarks
1	DCCB	1.0	May 2025	First Release

Approval History:

S. No.	Approver Name	Version Number	Date	Remarks
1	Board of Directors of Bank	1.0	May 31, 2025	First Release

Table of Contents

1. Policy Statement:

Mobile phones, as a medium for extending banking services, have attained greater significance because of their ubiquitous nature. The rapid growth of mobile users in India, through wider coverage of mobile phone networks, have made this medium an important platform for extending banking services to every segment of banking clientele in general and the unbanked segment in particular.

Mobile Banking like any other technology driven service channels come with risks inherent to the internet ecosystem. However, prudent users have found ways to manage these risks. Banks worldwide have moved their customers to the Smart Phones & Computers, with enormous gains in efficiency and service quality. Bank has to put in place secure and effective systems to mitigate risks from Bank's end. The customer must visualize the risks realistically and mitigate the same at their end. This includes proper handling of Username, passwords, Login and transaction PlN and overall safety of system at the user end.

2. Purpose:

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

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.

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. Approval / Review of the Policy:

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/ CISO.

c) As Mobile Banking is undergoing rapid changes at a faster pace, Mobile Banking Policy needs to be reviewed by IT Dept., 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 CISO for due consideration.

6. Deviations:

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 Policy, approval needs to be obtained from the competent authority/committee. Request for approval of deviation of Mobile Banking policy must provide the necessity for such amendment/addition/deletion.

7. Violations:

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.

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.

8. Eligible Accounts:

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

1. Savings Bank
2. Current Account

where:

a) Mode of operation for the accounts should be Individual/Self.
b) Account/s should be fully KYC compliant.
c) In case of joint accounts mode of operation is indicated as 'either or survivor' or 'anyone or survivor', or 'former or survivor'
d) In case of Partnership firm accounts where authorisation for operation is given to any one of the partners

9. Ineligible Accounts:

1. Joint accounts where mode of operation is other than 'either or survivor' or 'anyone or survivor', or 'former or survivor'
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 non-compliant accounts
8. Minor Accounts.
9. Acknowledgement of Debt (AOD) Expired loan accounts
10. NPA Accounts.
11. Overdrawn / Limit expired Accounts.

10. Services offered

a) Balance Enquiry
b) Mini Statement

c) Funds Transfer Intra Bank (Within DCCB)
d) Funds Transfer Interbank (To another Bank through NEFT)
e) Immediate Payment Services (IMPS)
f) Stop Payment of Cheque
g) Positive pay / Bill Payment through BBPS and tie up with Bill payment aggregators
h) Inquiry facility on Cheque Status
i) Debit card controls including Hot listing/Limit setting of ATM Cards
j) Green PIN generation/Set/Reset PIN for new debit cards

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

a) Mobile handset which supports Android application (Android Version 8.0 and above) /IOS
b) Active Mobile Number which is registered with only one customer ID of Bank.
c) Active ATM Card

- The customer desirous of availing mobile banking facility has to download the application from Google play store/apple store.
- All eligible accounts of the customer are displayed and customer has to select the primary account form the list of accounts.
- However customer can do transactions from all the registered accounts irrespective of whether the account is primary/secondary
- 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 analyse market trend / customer requirements and bring in changes in fund transfer limit / transaction limit under various categories.

Mobile Banking facility for the customer stands terminated during the following instances:

a) When the customer closes all his eligible accounts.
b) Mobile Number is changed
c) Customer himself wants to terminate the application

11. General Guidelines:

1. Bank customers should be on boarded to Mobile Banking, using registered Mobile Number.
2. Mobile Banking service can be provided to existing customer having saving account and Current account under proprietorship.
3. Mobile banking application should have SIM binding and device binding security control.
4. Registration of Mobile Banking can be completed using Debit Card, Branch Token and any other modes as decided by bank time to time.
5. Bank shall have a provision to block a Mobile Banking application/ service immediately on being informed by the customer through helpdesk numbers or Branches/offices and formalities, if any, can follow within a reasonable period
6. Transaction through Mobile banking shall have at least Two-factor authentication (2FA) control.
7. Mobile Banking application cannot be installed if any remote access tool like team viewer, any desk etc. are installed on mobile.
8. Mobile Banking application can only be registered on mobile network data.
9. The user information, password etc will be encrypted and will have restricted access to proper storage under advice of CSD /regulatory guidelines.
10. IT DEPT shall take up periodical review of registered users on MB database and take corrective action on deactivation/ deregistration of these users who have not utilized the app in last one year to avoid any misuse. Master Circular – Mobile Banking transactions in India – Operative Guidelines for Banks dated 01.07.2021 (Updated as on November 12, 2021)
11. IT DEPT shall issue comprehensive SOP for on-boarding of customer for Mobile Banking services, Registration of Mobile Banking, De-registration of Mobile Banking services, Change of Login and Transaction PIN, services on Mobile Banking, features of Mobile Banking, Transaction limit of Mobile Banking, Escalation matrix etc. and FAQs from time to time.

12. Roles & Responsibilities:

Branch:

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

In case of Partnership accounts, branch should ensure that partnership deed contains the clause related to operation of the obtain an undertaking from the partners duly authorising any one partner to operate the account for Mobile Banking purpose.

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 Login PIN (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.

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 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 Login PIN (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 Login PIN (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 suspects the misuse of the Login PIN (MPIN), customer should immediately initiate necessary steps to change the Login PIN (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 Login PIN (MPIN) is duly and legally authorized by the customer.

IT IM at Head Office:

IT IM at head office should assist IT DEPT in Hardware and software maintenance, vendor management. Conveying Bank's requirement to the concerned vendor, testing whether the product is working as per our requirement and implementation of services are the responsibilities of IT DEPT.

IT DEPT at 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 IT DEPT, HO.

13. Mobile Banking - Application features

DCCB Mobile app shall work on both data and Wi-Fi network; however, risk assessment shall be done by Risk Management Department from time to time. The DCCB Mobile app should adhere to the guidelines issued by RBI on mobile Banking/Internet Banking security controls dated 18.02.2021.

Mobile Banking – Transactions

All mobile banking transactions involving debit to the account shall be permitted only by validation through.

a) Two factor authentication (login pin & transaction pin- minimum 4-digit length)
b) One of the factors of authentication shall be Login PIN (MPIN) or any higher standard.
c) Where Login PIN (MPIN) is used, end to end encryption of the Login PIN (MPIN) is desirable.
d) The Login PIN (MPIN) shall be stored in a secure environment.
e) Additional authentication by way of OTP may also be explored.

Bank will set up suitable transaction limit in Mobile Banking as decided from time to time.

Security features

The Bank's Mobile Banking channels are to be protected by advanced security features, both physical and logical. Bank has to consider various risks inherent in transacting over a public network such as the internet and has deployed appropriate security measures to protect customers. Required security should be deployed to ensure safe and secure exchange of information between user Mobile Smart Phone and Banks Mobile application. Bank has to put in place secure and effective systems to mitigate risks from Bank's end. The customer must visualize the risks realistically and mitigate the same at their end. This includes proper handling of Username, passwords, Login and transaction PIN and overall safety of system at the user end.

Technology used for mobile banking should be secure and confirms to confidentiality, integrity, authenticity and non-repudiation.

The following security features should be implemented in the Mobile Banking System.

1. **Data Confidentiality**: Data and other information are kept highly confidential. This will not be disclosed to anybody unless legally warranted.
2. **Encryption**: Bank shall implement proper level of encryption and security at all stages of the transaction processing in Mobile Banking.

The endeavor shall be to ensure end-to-end encryption of the mobile banking transaction. Adequate safe guards would also be put in place to guard against the use of mobile banking in money laundering, frauds etc. Data and messages travel in SSL 128 bit end to end encryption while doing transactions online.

3. **Change password Option**: Customers are provided with an option to change the Login PIN (MPIN) and Transaction PIN (TPIN) at any number of times through application using Debit Card.
4. **Password confidentiality**:

   PIN is a 4-digit secret number/ code which is generated by the customer at the time of registering for mobile banking for the purpose of security. Login PIN (MPIN)s are known to the respective customers only. The Login PIN (MPIN)s are generated by the customer himself/herself and will not be known to any person in the bank. Login PIN (MPIN) is used to login into the mobile banking application and Transaction PIN (TPIN) is used while making any financial transaction or service request. Customers can also Reset/ change both the PIN through mobile banking after verifying their identity.
5. **Validity of Passwords**:

   a) There is no validity period for Login PIN (MPIN)

   b) The Mobile Banking Solution will also have the security features as available for Core banking solution.

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

   d) Login PIN and Transaction PIN are the two factors of authentication, when the transaction happens through Mobile Banking Application

      i. For resetting the Login PIN/Transaction PIN, option for the same is provided in the application for the customer.

      ii. Each Mobile Banking Transaction will have a unique Transaction ID which will enable us to track all types of transactions done through mobile banking.

      iii. 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 IT DEPT.

iv. Reporting tools/Reports are made available to track any transactions done through mobile banking.

Other Security Guidelines:

The following guidelines with respect to network and system security shall be adhered to:

a) Implement application-level encryption over network and transport layer encryption wherever possible.
b) Establish proper firewalls, intruder detection systems (IDS), data file and system integrity checking, surveillance and incident response procedures and containment procedures.
c) Conduct periodic risk management analysis, security vulnerability assessment of the application and network etc at least once in a year.
d) Maintain 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.
e) Implement appropriate physical security measures to protect the system gateways, network equipment, servers, host computers, and other hardware/software used from unauthorized access and tampering. The Data Centre of the Bank and Service Providers should have proper wired and wireless data network protection mechanisms

14. Mobile Banking -RBI Guidelines

The mobile Banking Policy will be governed by NABARD/RBI guidelines from time to time. Some of the major circulars issued by RBI are as under:

Reserve Bank of India (RBl) issued Master circular (DPSS.CO.PD.Mobile Banking. No.7107.73.001 /2014-15\ dated 01 .07.2014 and DPSS.CO.PD.Mobile Banking. No./2/02.23.001 /2016-2017 dated 01 .07.2016 containing rules / regulations / procedures prescribed to be followed by banks for operationalizing Mobile Banking in India.

Reserve Bank of India vide Master direction RBI/2020-71/74 dated 18.02.2021 provides necessary guidelines for the regulated entities to set up a robust governance structure and implement common minimum standards of security contorts for digital payment products and services. Under Chapter IV of the Master Direction, RBI has issued instructions applicable to Regulated Entities offering/ intending to offer mobile banking/mobile payments facility to their customers through mobile application.

Digital Payment Security Controls -Compliance of RBI Guidelines

RBI circular no. RBI 12070-21/74 DoS.CO.CS|TE.SEC.No.1852/3'1.01.015/2020-71, Dated 18.02.7021 on Master Direction on mobile Banking Security controls , provides necessary guidelines for the regulated entities to set up a robust governance structure and implement common minimum standards of security controls for digital payment products and services. As per the said circular, the provisions under this para shall be guided by the policy of the Bank. The contours of the policy, while discussing the parameters of any "new product" including its alignments with the overall business strategy and inherent risk of the product, risk management/ mitigation measures, compliance with regulatory instructions, customer experience, etc., should explicitly discuss about payment security requirements from Functionality, Security and Performance (FSP) angles such as:

a) Necessary controls to protect the confidentiality of customer data and integrity of data and processes associated with the digital product/ services offered;
b) Availability of requisite infrastructure e.g. human resources, technology, etc. with necessary back up;
c) Assurance that the payment product is built in a secure manner offering robust performance ensuring safety, consistency and rotted out after necessary testing for achieving desired FSP;
d) Capacity building and expansion with scalability (to meet the growth for efficient transaction processing);
e) Minimal customer service disruption with high availability of systems/ channels (to have minimal technical declines);

f) Efficient and effective dispute resolution mechanism and handling of customer grievance; and
g) Adequate and appropriate review mechanism followed by swift corrective action, in case any one of the above requirements is hampered or having high potential to get hampered.

The Board and Senior Management shall be responsible for implementation of this policy. The policy shall be reviewed periodically, at least on a yearly basis.

Mobile payments application security controls

In addition to the above controls, the following instructions are applicable to the banks offering/ intending to offer mobile banking/ mobile payments facility to their customers through mobile application:

1. On detection of any anomalies or exceptions for which the mobile application was not programmed, the customer shall be directed to remove the current copy/ instance of the application and proceed with installation of a new copy/ instance of the application. DCCB shall be able to verify the version of the mobile application before the transactions are enabled.

2. Specific Controls for mobile applications include:
   a) Device policy enforcement (allowing app installation/ execution after baseline requirements are met);
   b) Application secure download/ install;
   c) Deactivating older application versions in a phased but time bound manner (not exceeding six months from the date of release of newer version) i.e., maintaining only one version (excluding the overlap period while phasing out older version) of the mobile application on a platform/ operating system;
   d) Storage of customer data;
   e) Device or application encryption;
   f) Ensuring minimal data collection/ app permissions;
   g) Application sandbox/ containerization;
   h) Ability to identify remote access applications (to the extent possible) and prohibit login access to the mobile application, as a matter of precaution; and

i) Code obfuscation.

3. DCCB may consider to perform validation on the security and compatibility condition of the device/ operating system and the mobile application to ensure that activities relating to the account are put through the mobile application in a safe and secure manner.
4. DCCB may explore the feasibility of implementing a code that checks if the device is rooted/ jail broken prior to the installation of the mobile application and disallow the mobile application to install/ function if the phone is rooted/ jail broken.
5. Checksum of current active version of application shall be hosted on public platform so that users can verify the same.
6. DCCB shall ensure device binding of mobile application.
7. Considering that the additional factor of authentication and mobile application may reside on the same mobile device in the case of mobile banking, mobile payments, DCCB may consider implementing alternatives to SMS-based OTP authentication mechanisms.
8. The mobile application should require re-authentication whenever the device or application remains unused for a designated period and each time the user launches the application. Applications must be able to identify new network connections or connections from unsecured networks like unsecured Wi-Fi connections and must implement appropriate authentication/ checks/ measures to perform transactions under those circumstances.
9. The mobile application should not store/ retain sensitive personal/ consumer authentication information such as user IDs, passwords, keys, hashes, hard coded references on the device and the application should securely wipe any sensitive customer information from memory when the customer/ user exits the application.
10. DCCB shall ensure that their mobile application limit the writing of sensitive information into 'temp' files. The sensitive information written in such files must be suitably encrypted/ masked/ hashed and stored securely.
11. DCCB may consider designing anti-malware capabilities into their mobile applications.
12. DCCB shall ensure that the usage of raw (visible) SQL queries in mobile applications to fetch or update data from databases is

Avoided. Mobile applications should be secured from SQL injection type of vulnerabilities. Sensitive information should be written to the database in an encrypted form. Web content, as part of the mobile application's layout, should not be loaded if errors are detected during SSL/ TLS negotiation. Certificate errors on account of the certificate not being signed by a recognized certificate authority; expiry/ revocation of the certificate must be displayed to the user.

13. The device binding should be preferably implemented through a combination of hardware, software and service information.

15. Customer Awareness

a) The Bank may advise from time to time for up gradation of user system/ software, such as Mobile Banking application. Which are required for using mobile Banking services. There will be no obligation on the part of the Bank to support all the versions of user system/ software for accessing mobile Banking services of the Bank.

b) The Bank shall endeavor to provide Mobile Banking to user/ customer, such as 'inquiry about the balance in his/her account(s), details about transactions, statement of account, request for issue of cheque-books, request for transfer of funds between accounts of the same user and other accounts and many other facilities as the Bank may decide to provide from time to time. The Bank at its sole discretion may also make additions /deletions to the mobile Banking Services being offered, without giving any prior notices or reasons. The Bank shall take reasonable care to, ensure the security of and prevent unauthorized access to the mobile Banking Services using technology reasonably available. The user shall not use Mobile Banking services or any related service for any illegal or improper purposes.

c) Bank will endeavor to notify the user/customer through its website or through any legally recognized medium of communication found suitable by the Bank, regarding withdrawing/ suspending the Digital Payment Channel services wholly/ partially.

d) Bank will also endeavor to create awareness tips for using the mobile Banking applications, publish through social media videos about products/ features/ and security.

16. Grievance Redressal / Help Desk

Customer complaints / grievances arising out of mobile banking facility would be covered under the Reserve Bank – Integrated Ombudsman Scheme, 2021. Complaints raised by DCCB Mobile user's fraudulent transactions shall be reported to Fraud Monitoring Cell/ Committee to look into the frauds arising out of usage of digital channels. Mobile Banking transactions would also be covered under the RBI's notification RBI/7017-18/15 BD.No.Leg.BC.78l09.07.005/2017-18 dated July 6, 2017 on Customer Protection – Limiting Liability of Customers in Unauthorized Electronic Banking Transactions. Bank shall have proper Grievance Redressal mechanism and symmetrical escalation matrix as per Bank's Customer Service Policy. Bank shall have a help desk and disclose the details of the help desk and escalation procedure for lodging the complaints, on the websites.

17. Liability of the User and Bank

Customer Protection – Limiting Liability of Customers in Unauthorized Electronic Banking Transactions shall be strictly as per the RBI and Bank's defined policies.

18. Third Party Links

The Site may provide hyperlinks to other applications/ websites not controlled by DCCB and such hyperlinks do not imply any endorsement, agreement on, or support of the content, products and /or services of such websites. Bank don't editorially control the content, products and /or services on such mobile applications/ websites and shall not be liable, in any nature whatsoever, for the access to, or the inability to access to, or the use, inability to use or content available on or through such mobile applications/websites.

Any party (third party), desirous of creating a link to the Bank's mobile application / website, is required to obtain prior written approval of the Bank before doing so. The Bank may, at its absolute discretion, give or refuse to give such approval for linking the Bank's website. The Bank may at its

Absolute discretion rescind any approval granted and require the removal of any link to the Bank's mobile application/websites at any time. Any link to the Bank's mobile application /website must be made directly to the homepage of our website and "framing" or "deep-linking" of our website or content is strictly prohibited. Any use or display of the Bank's – logos, trade names, trademarks, web content or material in any form is not permitted except with the prior written approval of the Bank's ORMC. Limited liability of customers in unauthorized electronic Banking transaction shall be strictly guided by Customer services policy of the Bank.

19. Reference:

1. Reserve Bank of India in its circular No. RBl/2010-11/494-DBS.CO.lTC.BC.No/6/31.02.008/ 2010- 11 has categorically defined the Roles and Responsibilities of end user for electronic banking transactions.
2. RBI's notification RBI/7017-18/15 BD.No.Leg.BC.78l09.07.005/2017-18 dated July 6, 2017 on Customer Protection - Limiting Liability of Customers in Unauthorized Electronic Banking Transactions
3. Reserve Bank of India (RBl) Master circular (DPSS.CO.PD.Mobile Banking. No.7107.73.001 /2014-15\ dated 01 .07.2014 and DPSS.CO.PD.Mobile Banking. No./2/02.23.001 /2016-2017 dated 01 .07.2016 containing rules / regulations / procedures prescribed to be followed by banks for operationalizing Mobile Banking in India.
4. RBI circular no. RBI 12070-21/74 DoS.CO.CS|TE.SEC.No. 1852/3'1.01.015/2020-71 , dated 18.02.7021 on Master Direction on mobile Banking Security controls