KALLAPPANNA AWADE ICHALKARANJI JANATA SAHKARI BANK

Mobile Banking Policy

Document Control

KAIJSB Reference: **KAIJSB**
Document Title: **Mobile Banking Policy**
Document Version: **1.1.6**
Record No: **07**
Date: **22nd April 2025**

Change Record

Date	Author	Version	Change Reference
29th April 2017	KAIJSB Bank	1.1.0	Document Created
11th June 2020	KAIJSB Bank	1.1.1	Document Reviewed
10th May 2021	KAIJSB Bank	1.1.2	Document Reviewed
24th May 2022	KAIJSB Bank	1.1.3	Document Reviewed
8TH JUNE 2023	KAIJSB Bank	1.1.4	Document Reviewed
30TH AUGUST 2024	KAIJSB Bank	1.1.5	Document Reviewed
22nd April 2025	KAIJSB Bank	1.1.6	Document Reviewed

Distribution List

	Name
Master copy	CEO
Controlled Copy	IT Department
Online Copy	For all employees

	Developed by	Reviewed & Approved by
Name	IT Department	IT Department
Date	22nd April 2025	

TABLE OF CONTENTS

This policy has been framed considering RBI Circular no RBI/2014-15/104 DPSS.CO.PD. Mobile Banking. No. 2/02.23.001/2014-15 dated 01/07/2014 **and** NPCI guidelines.

1) POLICY STATEMENT :

"To gear up transaction banking for transforming and creating efficient banking service and enrich customer banking experience, the bank shall provide Mobile Banking facility to its customers."

The objective of this policy is to establish guidelines for the Bank's Mobile Banking Delivery channel. Mobile Banking is important due to the following:

- Enhances the Bank image and relevance in today's competitive Banking.
- Higher customer satisfaction and improved retention.
- Reduction in cost through migration to self service interactions.
- Reduction in Branch & ATM transaction volume and cost savings.
- Revenue opportunity with Merchant Services.
- Enhancement in security and consumer protection.
- Time consume & better efficient services.

2) DEFINATION:

The following words and expressions shall have the corresponding meanings wherever appropriate.

- **Applicant**: Applicant is the account holder applying for the mobile banking service provided by Kallappanna Awade Ichalkaranji Janata Sahakari Bank Ltd (KAIJS Bank).
- **Primary Account**: The account wherein the applicant is the first account holder.
- **Account number**: 15 digit account number as given by bank.
- **Customer**: The holder of a bank account in KAIJS Bank.
- **KAIJS Bank**: Kallappanna Awade Ichalkaranji Janata Sahakari Bank Ltd.
- **Base Branch**: The branch where the customer has his primary account.
- **Facility**: Mobile Banking facility provided to the customer for age limit above 18 year.
- **Application**: KAIJS Bank's Mobile Banking software (KAIJSMobile) downloaded in the mobile phone of the customer after registration.
- **Mobile Phone Number**: Mobile number that has been given by the customer to register for Mobile Banking Facility.

- **mPIN**: The personal identification number for doing transaction related to only own account/s using Mobile Banking Facility.

- **OTP**: One Time Password given by the system through SMS for doing fund transfer to the account of someone else or for merchant payments through Mobile Banking Facility.

- **IMPS**: Interbank Mobile Payment Services (IMPS) is an instant interbank electronic fund transfer service through mobile phones.

- **MMID**: Mobile Money Identifier (MMID) is a seven digit random number to be generated from the mobile application. MMID is required for fund transfer through IMPS mode.

- **USSD**: Unstructured Supplementary Service Data.

- **WAP**: Wireless Application Protocol.

- **GPRS**: General Packet Radio Service

3) REGISTRATION FOR MOBILE BANKING :

- Bank is fully computerized having core banking solution (CBS) and all branches are connected via own data center at Jaysingpur.

- Bank is strictly following all norms of Know your Customer (KYC), Anti Money Laundering (AML) and combating of financing of terrorism (CFT) issued by RBI from time to time.

- Bank is submitting all required reports to Financial Intelligence Unit – India (FIU-IND, Delhi).

- Bank is following all norms/condition by RBI & NPCI from time to time.

Bank is authorized for mobile banking via RBI permission letter no. RBI/2014-15/104 DPSS.CO.PD. Mobile Banking. No. 2/02.23.001/2014-15 and NPCI guidelines.

4) APPLICABILITY OF TERMS & CONDITIONS :

By using Mobile Banking Facility, the Customer thereby agrees to these Terms and Conditions, which form the contract between the Customer and KAIJS Bank. Mobile Banking Facility shall be governed by such terms and conditions as amended by KAIJS Bank from time to time. These terms and conditions shall be in addition to and not in derogation of other terms and conditions relating to any account of the Customer and/or the respective product or the service provided by KAIJS Bank unless otherwise specifically stated.

5) ADVANTAGES :

a) Greater customer convenience
b) Available by 24 X 7 days.
c) Reduce turnaround time and cost savings

d) Extensive application security
e) User friendly simple interface
f) Mobile banking having as edge over internet banking.
g) Available across the banks / across the world.

6) FUNCTION IN MOBILE BANKING :

a) Get money
b) Send Money
c) Payment of utility bills, DTH etc.
d) Other miscellaneous facilities in banking as provided in mobile banking application.
e) Other facilities from time to time.

7) PROCESS OF REGISTRATION OF MOBILE BANKING CUSTOMER:

- Customers who have applied for mobile banking can avail only this service.
- Bank shall formulate and implement a legally acceptable Application form for customers detailing the security requirements, customer responsibility, and customer acceptance etc. before providing access to the mobile banking delivery channel.
- Forms of mobile banking application will be made available at our all branches and also on our website in downloadable PDF format.
- Having the application form, perspective mobile banking customer may fill in the details along with their signatures and hand it over at their home branch.
- After a proper scrutiny, KYC compliance and signature verification our bank will register the application form in CBS software.
- Informed customer by mail or SMS.

8) GENERAL BUSINESS RULES GOVERNING MOBILE BANKING FACILITY :

The following Business Rules will apply to the facility being offered by KAIJS Bank:

- The facility will be available to customers having a satisfactory running Savings/Current/STOD/OD/CC/SOD/POD account with KAIJS Bank and completed the "Know Your Customer" (KYC) norms.
- The facility will not be offered to NRI / NRE Accounts, Minor accounts and Blind persons.
- KAIJS Bank reserves the right to reject a Customer's application for the facility without assigning any reasons.
- The applicant should personally submit the Mobile Banking Registration form to the base branch.
- KAIJS Bank shall suspend the registration of any Customer if the facility has not been accessed by the customer for a continuous period of one year (365 days). In such case,

customer/user has to uninstall the application and again reinstall the same and pass through the verification/validation process. After this, he/she can create new mPIN afresh.

- Entering wrong mPIN thrice will de-activate the facility. In such case, Customer has to re-register for the facility with his physical presence at the base branch.

- **Eligibility:**

Type of Account	Constitution	Mode of Operation	Who is Eligible
Saving Account (SB)	Single	Single	The Account Holder
		Either or Survivor	As per choice of all account holders. However, application is to be signed by all account holders.
	Joint	Jointly	**Not Eligible**
Current Account (CD and OD)	In the Name of Individual	Single	The Account Holder
	In the Name of Firm	Single	The Account Holder (All partners should Sign the application form and The notarized Consent Letter from all the partners of Partnership firm should be taken
		Jointly Operated	**Not Eligible**
CC/SOD/POD	Proprietorship, Partnership/ PVT. Ltd./Public Ltd/ Trust	Single	**BOD Resolution and Agreement should be made with bank for Pvt Ltd. Firm, Public ltd firm, trust, Partmentship accounts.**

- **Transaction Limit :** The daily upper cap per customer shall be Rs. 5,00,000/- for intrabank fund transfer, IMPS Transaction and Neft Transaction, bill payment and merchant payment when the service is used over the application /WAP.

- Daily transaction limit for NEFT is allowed upto Rs 10,00,000/- as per requested by customer as mentioned in Board resolution No. 16 dated 15/12/2017.

- Daily transaction limit for NEFT is allowed above Rs. 10,00,000 /- upto Rs. 50,00,000/- as per requested by customer in power of Chief executive officer of bank as mentioned in Board resolution No. 21 dated 16/10/2021.

- The customer can request for termination of the Facility by visiting the base branch and submitting the appropriate form for the said purpose. The Customer shall remain accountable for all transactions on the designated account made prior to confirmation of any such cancellation request.

- It shall be KAIJS Bank's endeavor to give a reasonable notice for withdrawal or termination of the facility, but KAIJS Bank may at its discretion withdraw temporarily or terminate the facility, either wholly or partially, anytime without giving prior notice to the customer. The facility may be suspended due to maintenance or repair work or any breakdown in the Hardware/Software or any emergency or for security reasons without prior notice and KAIJS Bank shall not be responsible for any loss/damage to the Customer.
- The services offered under the Facility will be automatically terminated if the primary account linked for the Mobile Banking Facility is closed. KAIJS Bank may also terminate or suspend the services under the Facility without prior notice if the Customer has violated the terms and conditions laid down by KAIJS Bank or on the death of the Customer when brought to the notice of KAIJS Bank or when prohibited by law or an order by a court or Authority or makes any fraud.

- It is mandatory to maintain sufficient balance as decided by bank from time to time to operate the mobile banking facility.

- The Cash Credit, SOD accounts are not eligible to avail Mobile Banking Facility, However the amount can be credited to such accounts from other accounts though mobile banking transaction.

9) USAGE OF FACILITY :

By accepting the Terms and Conditions while registering for the Facility, the Customer:

- Agrees to use Mobile Banking Facility offered by KAIJS Bank for financial and non-financial transactions, made available by KAIJS Bank under the Facility from time to time.

- Authorizes KAIJS Bank irrevocably to debit the Accounts which have been enabled for Mobile Banking Facility for all transactions/services undertaken using mPIN.

- Authorizes KAIJS Bank to map the Account Number, Customer ID and Mobile Phone Number for the smooth operations of the Facility offered by KAIJS Bank and to preserve the mapping record in its own server or server of any other third party and to use such data at its discretion for providing/enhancing further banking/technology products that it may offer.

- Agrees that he/she is aware and accepts that the Facility offered by KAIJS Bank will enable him/her to transact using mPIN within the prescribed limit and will be deemed as bonafide transactions and will not be disputed.

- Agrees that transactions initiated through Mobile Banking application are real time/instantaneous transactions and as such are irrevocable/ non-retractable. As such, Bank shall not entertain/accept any request for revocation of transaction or stop payment request for transactions initiated through Mobile Banking Facility at any stage.

- Understands and explicitly agrees that KAIJS Bank has absolute and unfettered right to revise the prescribed ceilings from time to time which will be binding upon him/her.

- Agrees to use the Facility on a mobile phone which is properly and validly registered in his/her name only with the respective Mobile Service Provider and undertakes to use the Facility

only through the mobile number which has been given at the time of registration of the Facility provided that the registered mobile number SIM has internet facility.

- Agrees that while the Information Technology Act, 2000 prescribes that a subscriber may authenticate an electronic record by affixing his digital signature which has been given legal recognition under the Act, KAIJS Bank is authenticating the Customer by using Mobile Number, mPIN &/or any other method like OTP etc decided at the discretion of KAIJS Bank which may not be recognized under the IT Act, 2000 for authentication of electronic records and this is acceptable and binding to the Customer and hence the Customer is solely responsible for maintenance of the secrecy and confidentiality of the mPIN/OTP without any liability to KAIJS Bank.

- Accepts that any transaction originating from his/her Customer ID and/or registered mobile phone number shall be assumed to have been initiated by the Customer and any transaction authorized by using his/her mPIN will be treated as duly and legally authorized by the Customer himself/herself.
- Agrees that the services offered under the Facility can be availed or accessed only from locations within the geographical boundaries of India due to security reasons.

- Understands and explicitly agrees that any change made by KAIJS Bank in terms and Conditions from time to time will be binding on us.

- Cash credit /SOD/POD account should be within drawing power and mobile banking transaction should be allowed only within drawing power accounts.

- Cash Credit/SOD/POD account period should not be expired and after expiry of account period, mobile banking facility should be immediately stopped.

- Stock statement should be submitted regularly, if not submitted mobile banking facility stop immediately.

- If borrower or guarantor expired , mobile banking facility should be immediately stopped.

- UPI facility not allow to CC/SOD/POD accounts.

- If fund transfer service is made available to the customer through the facility, it may be used for transfer of funds from account/s to other account belonging to third parties or customer himself maintained at the bank and / or at any other bank which falls under the network of Reserve bank in India's Electronic fund transfer or National Electronic Fund Transfer system or Real Time Gross Settlement or Immediate Payment Service or such other permissible medium. In such an event, the terms applicable to such facilities, in addition to this facility, shall be applicable. Bank has the right to impose limits/Cap on transaction (per transaction, daily, weekly, monthly) , transaction velocity limit, etc. as may be decided by the bank from time to time and such transaction limits shall be notified on the website of the bank.

10) RISK MANAGEMENT OF MOBILE BANKING:

Mobile banking provides many exciting new opportunities as well as create risk also to financial providers, carriers and the financial system. This new delivery channel holds out the prospect of adding new convenience for accessing banking and payment services to our customers. Especially for us, it may go even further to offer banking and payment services to those who have never

participated in the formal electronic banking system before. However, the use of mobile phones for mobile banking is relatively new and, as a consequence, the knowledge of the risk and the risk experience of providers is still limited.

For this reason, we have to assess Mobile banking risks and develop strategies to mitigate them on an ongoing basis.

Mobile Banking has unique characteristics that will increase our overall risk profile and the level of risks associated with traditional financial services, particularly

- ✓ Strategic
- ✓ Operational
- ✓ Legal
- ✓ Reputation risk
- ✓ Financial risk

These unique Mobile Banking characteristics include:

- ➢ Less face-to-face interaction with financial institution customers
- ➢ Dependence on third parties for necessary technical expertise
- ➢ Changing customer expectations
- ➢ Need to integrate Mobile Banking with the institution's legacy computer systems
- ➢ Proliferation of threats and vulnerabilities in publicly accessible networks
- ➢ Speed of technological change
- ➢ Increase visibility of publicly accessible networks (e.g. Internet)

11) VULNERABILITIES OF THE MOBILE CHANNEL:

Description	Commets
1) Relating to the mobile channel:	
(i) Encryption can be decrypted with sophisticated techniques, creating vulnerabilities at various points where data can be intercepted and read by third parties which may act on it.	Unauthorized information disclosure and transaction modification, replay and denial are covered by using sophisticated end-to-end encryption. The risks associated with the vulnerabilities can also be further mitigated by the introduction of appropriate procedures and controls.
2) **Relating to the mobile channel:**	
(i) Channel dependence: in the absence of widespread alternative channels, the risk of unavailable or unreliable service from the M-channel may be greater for users, for the provider, and even for the economy as a whole	The mobile network often goes where the internet, bank branches and ATMs do not necessary reach. Availability has two components – the coverage of the network and the actual availability when there is coverage. On the first issue mobile networks reach many places where there is no other form of electronic communication. On the second, there will be an assessment of the availability of the mobile banking services

	and if the availability is not sufficiently reliable, then the users will use it less and rely on cash more.
(ii) High volumes: the widespread penetration of phones and the rapid take up of some existing m-banking platforms suggests that the pressures on the system may be heightened by comparison with internet banking	The possibility of rapid adoption simply makes it more important that the risk factors are adequately considered upfront. In two areas – the capacity of the our bank's own systems and the congestion on the mobile Operators network. The ability of the mobile Operators to cope with the arrival of large numbers of financial transactions at its computer systems is usually where the bottleneck occurs and care must be exercised to ensure that the mobile banking channel has sufficient capacity to handle the m-banking transaction load. There will be many more voice calls, SMS and Data traffic that load the mobile networks than mobile banking transactions. Mobile banking transactions are usually a very small fraction of the overall mobile network load. (a SMS represents the equipment of about 0.1 seconds of speech on a GSM network). If the mobile network is no different to the internet, if the internet is overloaded due to heavy traffic then running a financial service through it will be problematic.
3) **Relating to the handset:**	
(i) Because the handset is more portable than say a laptop or PC, it is also more easily lost	Loss of handset does not compromise Mobile Banking unless combined with compromise of the owner's PIN (2 factor authentication)
(ii) The limited keypad functionality of standard handsets may effectively limit the choice of PINs, and/or resulting in PINs which can be compromised.	There is a difference between a PIN and password. Most PINs in practice are 4 or 5 digits long irrespective of what device is used for their entry. Combined with the fact that the access to the mobile banking is coupled to the possession of a specific SIM card the risk is no different to the possession of a credit card and a PIN for access to an ATM and the banking functions thereon.
(iii) The small screen of the handset limits the type and form of disclosure which can be made with financial transactions.	The usual 160 characters available in an SMS has provided sufficient to indicate transaction data – namely source and destination accounts, amount, reference numbers, remaining balance and time and date. For detailed conditions of service – these need to be made available physically.
4) **Relating to m-payment application:**	

(i) Since these networks are often out-sourced, the interface with the mobile network provider may create additional vulnerabilities.	While true, this is no different from e-banking environments and their connection to web servers and the internet. The interface is the place where all the transactions pass and thus usually is a point of high risks.

12) TECHNOLOGY AND SECURITY STANDARDS:

Our overall security framework will ensure the following.

- ✓ Encrypted (minimum encryption standard will be min 128 bit SSL) messaging/ session between consumer's phone and third party service provider / telecom company.
- ✓ All subsequent routing of messages to our mobile banking serves will be with the highest level of security with dedicated connectivity like leased lines/ VPNs.
- ✓ If any sensitive information is stored in third party systems, we will ensure that access to this information is restricted with appropriate encryption and hardware security standards.
- ✓ All transactions that effect an account (those that result in to an account being debited or credited, including scheduling of such activity) will be allowed only after authentication of the mobile number and the mPIN associated with it.
- ✓ mPIN number will not allowed to be stored in the mobile banking application on the phone.
- ✓ All accounts, credit or debit cards allowed to be transacted through the mobile phones will have the mobile phone number linked to the account, credit or debit card. This mobile number will be used as the second factor authentication for mobile transaction.
- ✓ During the transaction, the PIN will not travel in plain text.
- ✓ Min 128 bit SSL, encryption will be implemented for communication from the mobile handset to the mobile payments service provider's server.
- ✓ Proper system of verification of the phone number will be implemented, wherever possible. This is so as to guard against spoofing of the phone numbers as mobile phones would be used as the second factor authentication.
- ✓ The payment authorization message from the user's mobile phone will be securely encrypted and checked for tampering by the service provider or the bank. It will not be possible for any interceptor to change the contents of the message.
- ✓ Our Bank Data Center is ISO 27001:2005 certified for Information Security Management System i.e. Data center, DR Site and ATM Card Management. And has a security policy duly approved by the board of directors. In Policy we have a security organization with segregation of duty of chief information security officer dealing exclusively with information systems security and information Technology Division which actually implement the computer systems. We have a network and database administrator with clearly defined roles.
- ✓ Our Bank has introduced logical access controls to data, systems, application software, utilities, telecommunication lines, libraries, system software, etc. Logical access control techniques include user-ids, password and biometric access technologies.
- ✓ Our Bank has implemented carefully designed Networks with Firewall, Routers, and Switches etc. and also undergoes an annual system audit done by a qualified, certified and Cert-in certified agency.
- ✓ Periodically our CISA audit is conducted by certified Information System Auditors and the information system auditors monitors periodic penetration tests of the system, which

include:

- Attempting to guess passwords using password cracking tools.
- Search for back door traps in the programs.
- Attempt to overload the system using DDoS (Distributed Denial of Service) and DoS (Denial of Service) attacks.
- Checks for commonly known holes in the software, especially the browser and the e-mail software.
- The penetration testing are also carried out by engaging outside 'Ethical Hackers'

✓ Our Bank has proper infrastructure and schedules for backing up data. The backed-up data is periodically tested to ensure recovery without loss of transaction in a time frame as given out in the bank's security policy.

✓ Bank has hosted DR site at TJSB Bank, Pune for Business Continuity Plan (BCP).

13) BUSINESS & LEGAL ISSUES :

- Considering the legal position prevalent, there is an obligation on us to not only establish the identity but also to make enquiries about integrity and reputation of the prospective customer. Therefore, even though request for opening a saving / current account can be accepted over Mobile Telecommunication, there will be opened only after proper introduction and physical verification of the identity of the customer.
- From a legal perspective, security procedure adopted by us for authenticating users is recognized by law as a substitute for signature.
- Under the present laws and regulations there is an obligation on us to maintain secrecy and confidentiality of customers accounts. In the Mobile Banking scenario, the risk of banks not meeting the above obligation is high on account of several factors. Despite all reasonable precautions, banks may be exposed the enhanced risk of liability to customers on account of breach of secrecy, denial of service etc., because of hacking/ other technological failure.
- The Consumer Protection Act, 1986 defines the right 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. Considering the banking practice and rights enjoyed by customers in traditional banking, bank's liability to the customers on account of unauthorized transfer through hacking, denial of service on account of technological failure etc. needs to be continuously assessed and we should consider insuring ourselves against such risks.

14) MISCELLANEOUS

- The Customer shall be required to get acquainted with the process for using the Facility and that he/she shall be responsible for any error made while using the Facility.
- KAIJS Bank reserves the right to decide what services may be offered under the Facility. Additions/deletions to the services offered are at its sole discretion.
- The instructions of the Customer shall be effected only after authentication under his/her Customer ID and mPIN or through any other mode of verification as may be stipulated at the discretion of KAIJS Bank.
- While it shall be the endeavor of KAIJS Bank to carry out the instructions received from the Customer promptly, it shall not be responsible for the delay/failure in carrying out the instructions due to any reasons whatsoever including failure of operational system or due to any requirement of Law. The Customer expressly authorizes KAIJS Bank to access his/her

account information required for offering the services under the Facility and also to share the information regarding his/her accounts with the service provider/third party as may be required to provide the services under the Facility.

- The transactional details will be recorded by KAIJS Bank and these records will be regarded as conclusive proof of the authenticity and accuracy of transactions.
- The Customer hereby authorizes KAIJS Bank or its agents to send promotional messages including messages related to the products of KAIJS Bank, greetings or any other messages KAIJS Bank may consider from time to time.
- The Customer understands that KAIJS Bank may send rejection or 'Cannot process the request' messages for the service request(s) sent by the Customer which could not be executed for any reason.
- KAIJS Bank shall make all reasonable efforts to ensure that the customer information is kept confidential but shall not be responsible for any inadvertent divulgence or leakage of customer information for reasons beyond its control or by action of any third party.
- The Customer expressly authorizes KAIJS Bank to carry out all requests/transactions purporting to have been received from his/her mobile phone and authenticated with his/her mPIN. All fund transfer/payment transactions, initiated from the customer's registered mobile phone using his/her mPIN, will be treated as bonafide transactions expressly authorizing KAIJS Bank to effect the fund transfer/to make the payment.
- The Customer shall be responsible for the safe custody and security of the Mobile Banking application downloaded on his/her mobile phone to avoid unauthorized usage. It is the responsibility of the Customer to advise KAIJS Bank of any loss or theft of mobile phone by adopting the procedure laid down by KAIJS Bank for the purpose. The Customer shall solely remain responsible and accountable for all transactions which may take place from the stolen/lost mobile phone on the designated account prior to confirmation of request for de-registration from KAIJS Bank.
- The Customer understands that he/she shall be required to initiate SMS/ USSD/ GPRS/WAP services for availing Mobile Banking facility and hence shall be liable to pay charges to his/her respective Service Provider as per applicable tariff plan. The Customer also understands that KAIJS Bank will neither be responsible/ liable for any such charges levied by the Service Provider nor is liable for any dispute that may arise between such telecom service provider and the Customer.
- It is the responsibility of the Customer to disclose his/her non residency status to the base branch in case there is change in residence status of the customer.
- The customer confirms that the KAIJS Bank shall not be held liable or responsible for any delays/deficiencies in settlement of a transaction due to handset / or technical issues.
- Board of Resolution should be signed by all the directors not only authorized signatory.
- Relevant undertaking will be taken mentioned therein, that , the account holder or guarantor will have sole responsibility to inform bank about mobile no holder is deceased or mobile is lost, it is customer responsibility to inform immediately to bank and stop the mobile banking immediately.

15) FEE STRUCTURE FOR THE FACILITY :

At present, KAIJS Bank does not charge any fee for offering this Mobile Banking Facility. KAIJS 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. Display of such charges on Bank's website would serve as sufficient notice and the same is binding on the customers.

16) ACCURACY OF INFORMATION :

a. It is the responsibility of the Customer to provide correct information to KAIJS Bank

through the use of the facility or any other method. In case of any discrepancy in information, the Customer understands that KAIJS Bank will not be in any way responsible for action taken based on the information. KAIJS Bank will endeavor to correct the error promptly wherever possible on a best effort basis, if the Customer reports such error in information.

b. Customer understands that KAIJS Bank will try, to the best of its ability and effort, to provide accurate information and shall not hold KAIJS Bank responsible for any errors or omissions that may occur due to reasons beyond the control of KAIJS Bank.
c. Customer accepts that KAIJS Bank shall not be responsible for any error which may occur in spite of the steps taken by KAIJS Bank to ensure the accuracy of the information and shall not have any claim against KAIJS Bank in the event of any loss/ damage suffered as a consequence of an inaccurate information provided by KAIJS Bank.

17) RESPONSIBILITIES & OBLIGATIONS OF THE CUSTOMER :

a. The Customer will use offered facility using the mPIN in accordance with the procedures laid down by KAIJS Bank from time to time.
b. The Customer shall keep the customer ID, mPIN and OTP confidential and will not disclose these to any other person. He/she will not record the same in a way that would comprise the security of the facility. In case of using the facility by making use of SMS based system the Customer will take utmost precaution to delete the SMS stored in sent folder of the mobile phone, which may have mPIN in readable form.
c. The Customer will be responsible for all transactions, including fraudulent/erroneous transactions made through the use of his/her mobile phone, SIM card and mPIN, regardless of whether such transactions are in fact entered into and /or authorized by him/her or not. The Customer will be responsible for the loss/damage, if any suffered.
d. The Customer will ensure that his/her mobile phone is not shared with anyone under any circumstances and shall take immediate action to de-register from Mobile Banking Facility as per the procedure laid down, in case of misuse or theft or loss of the mobile phone or SIM card.
e. The Customer will be totally responsible for notifying KAIJS Bank immediately if he/she suspects the misuse of the mPIN by some other person. He/she will initiate the necessary steps immediately to change his/her mPIN. In such case, a customer only will be accountable for all the transactions done using his/her mobile phone and misusing the mPIN, even during the period from notifying KAIJS Bank till mPIN is changed, no doubt it will be always Bank's endeavor to facilitate the change of mPIN at the earliest.
f. The Customer shall always be liable for all loss incurred by him/her or by KAIJS Bank on breach of any of the Terms and Conditions contained herein by him/her or contributed or caused the loss by his/her direct/indirect deliberate /negligent actions/inactions any time.
g. The Customer shall be liable and responsible for all legal compliance and adherence of all commercial terms and conditions in respect of the mobile connection/SIM card/ mobile phone through which the facility is availed and KAIJS Bank does not accept/acknowledge any responsibility or even entertain any communication in this regard.
h. The Customer shall be prudent in downloading any content through bluetooth or uploading/installing any other software/ programs /game/ music files/ application received through trusted or un-trusted source and ensure that proper anti-virus software is used from time to time to remove malware residing in the handset.
i. It shall be KAIJS Bank's endeavor to provide proper Mobile Banking Application compatible with

the Customer's mobile phone, however KAIJS Bank will not be responsible in some exceptional cases where the mobile banking application may not be compatible with or does not work on the mobile handset of the customer.

18) CUSTOMER AWARENESS :

All the terms and conditions related to customer will be displayed on websites. Important conditions will also be written on application form. Copy of policy will be placed at head office and customer can access it on giving written application. The Customer shall keep himself /herself updated with regard to any information/ modification relating to the services offered under the Facility which would be publicized on the website and would be responsible for the same.

19) INDEMNITY:

In consideration of KAIJS Bank providing the Facility, the Customer agrees to indemnify and hold KAIJS Bank harmless against all actions, claims, demands proceedings, loss, damages, costs, charges and expenses which KAIJS Bank may at any time incur, sustain or be put to as a consequence of or arising out of or in connection with any services provided to the Customer pursuant hereto. The Customer shall indemnify KAIJS Bank for unauthorized access by any third party to any information/instructions/triggers given by the Customer or breach of confidentiality.

20) RIGHT TO CHANGE THE POLICY :

Bank reserves the right to change the policy as per guidelines issued by RBI from time to time.

Asst General Manager
IT Department

Asst General Manager
IT Department

Chief Compliance Officer

General Manager

BOARD MEETING RESOLUTION NO. 8/9 DATED 30 / 04/ 2025

FOR KALLAPPANNA AWADE ICHALKARANJI JANATA SAHAKARI BANK LTD.

CHIEF EXECUTIVE OFFICER

CHAIRMAN