THE BHAGYALAKSHMI MAHILA SAHAKARI BANK LTD; NANDED

Privacy Policy

Bhagyalakshmi Mahila Sahkari Bank Ltd. Nanded is committed to ensuring that your privacy is protected. Should we ask you to provide certain information by which you can be identified when using this website, then you can be assured that it will only be used in accordance with this privacy statement. This Privacy Policy provides an explanation as to what happens to any personal data that you provide to us, or that we collect from. We may change this policy from time to time by updating this page. You should check this page from time to time to ensure that you are happy with any changes.

This policy is effective from February 2022.

OBJECTIVE

a. To ensure the security and privacy of customers' sensitive personal data.

b. To comply with the Privacy Regulations viz. The information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules, 2011).

c. Follow good practice.

d. Protect Bank's Stake holders, staff and other individuals

e. Protect the organization from the consequences of a breach of its responsibilities

Security and confidentiality of Customer Data

1. 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.
2. 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.
3. 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.
4. 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.
5. 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.
6. 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.
7. 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.

8. 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.

Storing Your Personal Data

Data that is provided to us is stored on our secure servers. Details relating to any transactions entered into on our site will be encrypted to ensure its safety.
The transmission of information via the internet is not completely secure and therefore we cannot guarantee the security of data sent to us electronically and
transmission of such data is therefore entirely at your own risk. Where we have given you (or where you have chosen) a password so that
you can access certain parts of our site, you are responsible for keeping this password confidential.

Disclosing Your Information

Where applicable, we may disclose your personal information to any member of our group. We may also disclose your personal information to third
parties:

Customer liability in cases of unauthorized electronic banking transactions:

In spite of all the efforts, if any unauthorized electronic transaction takes place in the customer's account, the customer should
inform the Bank immediately by any of the following means -

By calling bank's free helpline no. 02462 248066
By personally reporting to home branch during working hours of the Branch.

On receipt of report of an unauthorized transaction, the Bank will take immediate steps to prevent further unauthorized transactions in the account.

LIMITED LIABILITY OF CUSTOMER

A customer shall be liable for the loss occurring due to unauthorized transactions in the following cases:
In cases where the loss is due to negligence by a customer, such as where he has shared the payment credentials details namely viz, internet banking user id /PIN, Debit Card PIN/OTP or due to improper protection on customer devices like mobile/ laptops/desktops leading to malware/Trojan or phishing/vishing attacks, the customer will bear the entire loss incurred until he/she reports the unauthorized transaction to the bank. Any loss occurring after the reporting of the unauthorized transaction shall be borne by the bank.

In cases where the responsibility for the unauthorized electronic banking transaction lies neither with the bank nor with the customer, but lies elsewhere in the system and the customer notifies the bank of such a transaction and when there is a delay beyond three working days in reporting by the customer,i.e if a customer notifies the Bank within 4 to 7 working days of receiving a communications of the transaction, the per transaction liability of the customer shall be limited to the transaction value or the amount as shown below in table,
whichever is lower.

Maximum liability of a customer under paragraph 6.4

Type of account Maximum liability (Rs.)

? Basic Savings Bank Deposit Account	5000
? All other Savings Bank accounts	10000
? Current / Cash Credit / Overdraft accounts of individuals with average balance (during 365 days preceding the incidence of fraud) / limit up to Rs. 25 lakh	10000
? All other Current / Cash Credit / Overdraft Accounts	25000

Customer obligations :

Customer shall mandatorily register valid mobile number with the Bank.

Customer shall regularly update his /her registered contact details as soon as such details are changed. Bank will only reach out to customer at the last known email/ mobile number. Any failure of customer to update the Bank with changes shall be considered as customer negligence. Any unauthorized transaction arising out of this delay shall be treated as customer liability.

Customer should provide all necessary documentation – customer dispute form, proof of transaction success/ failure and should also file a police complaint and provide copy of the same to the Bank.

Customer should co-operate with the Bank's investigating team and provide all assistance

Customer must not share sensitive information (such as Debit, PIN, CVV, Net-Banking Id & password, OTP, transaction PIN, challenge questions) with any entity, including bank staff.

Customer must protect his/her device as per best practices and update latest antivirus software on the device (Device includes smart phone, feature phone, laptop, desktop and Tab)

Customer shall go through various instructions and awareness communication sent by the bank on secured banking

Customer must set transaction limits to ensure minimized exposure.

Customer must verify transaction details from time to time in his/her bank statement and raise query with the bank as soon as possible in case of any mismatch.

Customer should attend training / awareness programs conducted by the bank.

FORCE MAJEURE:

The bank shall not be liable to compensate customers for delayed credit if some unforeseen event including but not limited to civil commotion, sabotage, lockout, strike or other labour disturbances, accident, fires, natural disasters or other "Acts of God", war, damage to the bank's facilities or of its correspondent bank(s), absence of the usual means of communication or all types of transportation, etc. beyond the control of the bank prevents it from performing its obligations within the specified service delivery parameters.