

## **1 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 BNSB's Stake holders, staff and other individuals
- e)Protect the organization from the consequences of a breach of its responsibilities

## **2 SCOPE AND APPLICABILITY**

This policy is applicable to all employees of the BNSB, Head office and its branches and its vendors.

## **3 POLICY**

Bank customers' sensitive personal data i.e. biometric data, passwords and financial information such as bank account details, credit and debit card details shall be protected by BNSB by following reasonable security practices and procedures. For this, BNSB has:

- Adopted a comprehensive documented information security program and policies that contain managerial, technical, operational and physical control measures
- Implemented the documented security practices
- Information Systems audits of Bank's Data Center and branches conducted every year

BNSB shall always:

- a) Comply with both the law and good practices
- b) Respect individual's rights of non-disclosure, confidentiality.
- c) Be open and honest with individuals whose data is held.
- d) Provide training and support for staff and volunteers who handle personal data, so that they can act confidently and consistently
- e) Recognise that its first priority is to avoid causing harm to individuals, which means:
  - keeping information securely in the right hands, and
  - holding good quality information.

IS Policy No. 11 Version : 1.0 Date : 14.03.2023	<b>Data Privacy Policy</b>	BNSB, Pune
--	----------------------------	------------

<b>3.1</b>	<b>Security and confidentiality of Customer Data</b>
<b>3.1.1</b>	As per Information Systems security policies and procedures implemented in the BNSB, BNSB 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.
<b>3.1.2</b>	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.
<b>3.1.3</b>	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.

<b>3.2</b>	<b>Data Usage</b>
<b>3.2.1</b>	Bank shall use customers' personal data only for the purpose for which it is collected. Bank is committed to ensuring that personal data is kept strictly confidential. However, personal data may be disclosed to regulatory authorities for the purposes of obtaining regulatory approval in accordance with applicable legal requirements, or otherwise to comply with applicable legal requirements.

<b>3.3</b>	<b>Data Retention</b>
	Customer's data shall be retained as per Senior management Directives (circulars issued by Head Office) and Regulatory Standards (RBI directives).

IS Policy No. 11 Version : 1.0 Date : 14.03.2023	<b>Data Privacy Policy</b>	BNSB, Pune
--	----------------------------	------------

<b>3.4</b>	<b>Data modification</b>
	BNSB shall update the customer data only after ensuring the authenticity of the change request. Adequate access controls and authorization controls shall be in place to monitor data modifications.
<b>3.5</b>	<b>Data Quality</b>
	BNSB shall continuously review and asses the quality and completeness of the data.
<b>3.6</b>	<b>Auto Read OTP functionality:</b>
	BNSB shall have auto read facility for OTP validation in the Mobile application. Whenever the OTP is send to the customer, BNSB mobile application shall auto populate the OTP in the required field instead of entering by keypad.
<b>3.7</b>	<b>SMS forwarding App / Remote access App:</b>
	BNSB mobile application shall 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 applications, BNSB mobile application shall restrict the users to access the login to the BNSB mobile application if user have installed the listed apps.
<b>3.8</b>	<b>SMS Delivery status facility:</b>
	BNSB shall confirm that SMS Service Provider shall have Call back facility available to verify the status of SMS send from mobile application, also SMS service provider shall have “SMS Delivery receipt check” to know the delivery status of the SMS forwarded from mobile application end.
<b>3.9</b>	<b>SMS forwarding App / Remote access App</b>
	BNSB 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 in case of any listed application with likes of “Remote Access Applications” and “SMS Forwarder Applications” is detected.
<b>3.10</b>	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.
<b>3.11</b>	<b>SECURITY AWARENESS AMONG USERS:</b>
	All staff handling personal data shall receive training in the requirements of data protection related laws and regulations. They shall also be educated about the legal consequences of intentional / unintentional disclosure /leakage of customers’ data.
<b>3.12</b>	The Bank shall take written consent of the customer in specific format before providing any special services via mobile.

-----