Data Privacy Policy	Swami Swaroopanand Sahakari Patsanstha (SSSP)Ratnagiri

1. **OBJECTIVE –**

a) To follow data privacy good practises.
b) Protect the organization from consequences of a breach of its responsibilities.
c) To ensure the security and privacy of customer's data
d) Protect stake holders, staff and other individuals.
e) To comply with Privacy Regulations viz. The information Technology(Reasonable Security Practises and Procedures and Sensitive Personal Data or Information Rules, 2011)

2. **SCOPE AND APPLICABILITY –**

This policy is applicable to all employees of the SSSP and its branches and its vendors and HO.

3. **POLICY –**

Customer's sensitive personal data shall be protected by SSSP i.e. biometric data, passwords and financial information of bank account details. For this SSSP has:

a) Information Systems audits of SSSP's Data Centre and Branches conducted every year.
b) Adopted a comprehensive documented information security programme and policies. It contains managerial, technical, operational and physical control measures.
c) Implemented the documented security practices.

SSSP shall always:

- Comply with both the law and good practises
- Be open and honest with individuals whose data is held.
- Respect individuals rights of non disclosure, confidentiality
- 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.
- Provide training and support for staff and volunteers who handle personal data, so that they can act confidently and consistently.

3.1	**Security and Confidentiality Data of Customer**
3.1.1	As per Information Systems security policies and procedures implemented in the SSSP, SSSP has implemented administrative, physical and technical safeguard to protect electronic personal data from loss, misuse and unauthorized access. Customer's personal data shall be stored on a secured database.
3.1.2	SSSP shall not sell personal data to any third party or anybody and shall remain fully compliant with confidentiality of the data as per law
3.1.3	SSSP shall share customer's 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.

3.2	**Usage of Data**
	SSSP shall use customer's personal data only for the purpose for which it is collected. SSSP 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.

3.3	**Auto Read OTP Functionality**
	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 the keyboard.

3.4	**SMS Forwarding App/Remote access App**
	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.

3.5	**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 he delivery status of the SMS forwarded from our end.

3.6	**Data Retention**
	Customers data shall be retained as per Senior management Directives(circulars issued by Head Office) and Regulatory Standards(RBI Directives)

3.7	**Modification of Data**
	SSSP 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

3.8	**Quality of Data**
	SSSP shall continuously review and asses the quality and completeness of the data

3.9	**Security Awareness Among Users**
	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 customer’s data.

Record of Revisions:

Rev. No.	Date	Changes	Remarks
1	15 Jan 2023		Draft Approval

Record of Approval:

Rev. No.	Prepared by	Reviewed by	Approved by
Name	IT Dept	IT Committee	BOD
Designation	IT Head	Manager	
Date	09 JAN 2023	11 JAN 2023	15 JAN 2023