

1 OBJECTIVE

- To ensure the security and privacy of customers' sensitive personal data.
- To comply with the Privacy Regulations viz. The information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules, 2011).
- Follow good practice.
- Protect ICBL's Stake holders, staff and other individuals
- Protect the organization from the consequences of a breach of its responsibilities.

2 SCOPE AND APPLICABILITY

This policy is applicable to bank's information about customer and business process in the form of media, documents and publish on web-site and employee of the Head Office and 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 ICBL by following reasonable security practices and procedures. For this, ICBL 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

ICBL shall always:

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

3.1 Security and confidentiality of Customer Data

- As per Information Systems security policies and procedures implemented in the ICBL, ICBL 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.
- 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.
- 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.

3.2 Data Usage

- 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.

3.3 Data Retention

- Customers data shall be retained as per Senior management Directives (circulars issued by Head Office) and Regulatory Standards (RBI directives).

3.4 Data modification

- ICBL 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.

3.5 Data Quality

- ICBL shall continuously review and assess the quality and completeness of the data

3.6 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 customers' data.
-