**3.14 Security and confidentiality**

The safe handling of Data is essential to ICICI Bank's continuing operation, particularly as the business expands. The modern business environment requires ever more robust systems to ensure the security of Personal Data, and the implementation of such systems is a vital tool in the management of our business. By keeping Personal Data secure we protect the interests of the business, itS employees and its customers.

The Bank has an obligation to ensure that appropriate security measures are put in place to protect personal information against unauthorised and unlawful processing, accidental lost, destruction, misuse, disclosure or corruption.

Employees are responsible to ensure that personal information is held securely and is not disclosed to any unauthorised third party.

Maintaining data security means guaranteeing the confidentiality, integrity and availability of personal data, defined as follows:

* confidentiality means that only people who are authorised to use the data can access it;
* integrity means that personal data should be accurate and suitable for the purpose for which it is processed; and
* availability means that authorised users should be able to access the data if they need it for authorised purposes.

Access to information and computer systems shall be on a strictly "need to know" basis, and the level of security that should be applied to confidential information, including personal data, will vary with the sensitivity of information in question.

Each business area must ensure that its electronically stored Personal Data is secure. Access must be restricted and files should be password-protected as appropriate.

Personal Data stored in paper form must be kept secure. It must be stored in lockable cabinets with possession of keys controlled and restricted as appropriate. Contracts with off-site archive facilities must contain adequate measures to ensure security and confidentiality.   
  
Refer the updated Information Security Policy of the Bank for further guidance on data security and confidentiality measured adopted by the Bank, available on Bank's Intranet.

**Data MIS requests to BIU and use of Hot Folder**

The Bank has Seclore based file encryption system as an automated process for transfer of data files from BIU server in India to a folder hosted in UK File Server. All staff members requiring simple read access need not install any Seclore client software for accessing data shared by BIU. However in case there are requirements to modify, delete and forward / store data, employees would need to install Seclore client.. Additionally, ICICI Bank UK has created a 'Hot Folder' on shared drive (172.24.40.27) with the name "Seclore\_UK" Any file placed in this folder will be Seclore protected. All staff members must use this folder to save the data generated irrespective of its source i.e. BIU, sales CRM, branch generated, etc.

Further, as per the process defined under the DPIA process, any data request being sent to BIU which includes personal data of customers needs to be first sent for approval to the DPO. Employees should attach the approval received from DPO when raising a Service Request (SR) in the system for BIU to extract the data. BIU to act on the SR upon verification of DP0 approval.

Refer Appendix 4 on the process note for accessing customer data internally.

**Test Data**

Live Data should not be used in systems testing unless unavoidable and with the knowledge and prior consent of IT Security and the Data Protection Officer.