

## **Privacy Policy**

### **OBJECTIVE**

The Objective of this Policy is to ensure privacy of the information about its' customers received / obtained by the company in any form – electronic and / or otherwise.

### **SCOPE**

The policy covers information received / obtained by the company about customers in electronic as well as any other forms like paper etc. The policy also covers information received / obtained by the Company through other sources like received from any Financial Institution during the normal course of business such as Statement of account / holding statement, etc.

This policy covers information handling infrastructure like the Hardware, applications, Databases, Operating Systems, Network Assets, any electronic / non electronic device and oral information sharing.

This policy sets out the basis on which information received / obtained by the company is processed by the Company Privacy policy.

### **DESCRIPTION**

As a part of Company's commitment to the customers and regulatory requirements, it shall be ensured that privacy of the information received about the customers is maintained which means that it is used properly and kept securely.

### **Definitions**

- Customer – The person / institute / organization / group of persons which intends to take or is taking services of the Company.
- "Personal information" means any information that relates to The Company's Customers, which either directly or indirectly, in combination with other information available or likely to be available with the Company and is capable of identifying such Customer. Personal Information may include Customer's name, age, gender, contact details, email addresses, passport number, Income, PAN, details of nominees, account numbers, types of accounts, type of relationship with Company, financial information, physical, physiological and mental health condition, Biometric information, any detail relating to the above clauses as provided to Company for providing services, and any of the information received by the Company for processing, stored or processed under lawful contract or otherwise and other information that may directly or indirectly identify a particular Customer.

- Any information that is freely available or accessible in public domain or required to be furnished under the Right to Information Act, 2005 or under any other law for the time being in the force shall not be regarded as Personal Information for the purpose of this policy.
- "Processing" means any operation or a set of operations whether carried out by automatic means or not that relates to
  - The organization, collation, storage, updating, modification, alteration or use of personal data
  - The merging, linking, blocking, degradation, erasure or destruction of personal data
- "Privacy" means confidentiality of the Personal information of the Customer of the Company
- "Sensitive Personal Information" - As defined under the IT Act 2000 and rules made there under.

### **Collection of Personal Information**

- The Company shall collect Personal Information, as may be required in the normal course of business and permitted by laws and regulations.
- If the Company collects other Personal Information, in order to provide better services, the same also shall be classified as "Personal Information" as defined in this policy.
- Personal Information shall not be collected unless it is necessary or collected for a lawful purpose or connected with a function or activity or business of the Company.
- The Company may also collect information relating to -
  - Visits to company website, but not limited to traffic data, location data, web logs, etc.
  - Information from third parties such as peers, friends, relatives, etc.
  - Computer used by the Customer, including IP address, operating system and browser type, for system administration and share the same with third parties. This is statistical data and may not identify any individual.

- The Customer's general internet usage by using a "cookie file" which is stored on the hard drive of the Customer's computer. This data also may not identify any individual.
- Following precautions shall be taken while collecting Personal Information to ensure that the Customer understands:
  - That Personal Information is being collected
  - The purpose for which the information is being collected.
  - Relevant details like the name of the person collecting information on behalf of the Company and the manner in which this information shall be retained.
  - While collecting Personal Information, the Customers shall be given an option to decline providing Personal Information. However, in such cases the Customers shall be clearly informed that they shall not be entitled to certain services or products for which such Personal Information is required.
- If the Customer provides Personal Information initially and later decides to withdraw the Personal Information, it shall be clearly informed to such Customer that though the Company shall return the Personal Information, certain services or products for which such Personal Information was required shall be discontinued.
- Personal Information shall not be retained for period which is longer than the required for the purpose for which it was collected.

### **Storing of Personal Information**

- Once Personal Information is collected from the Customers, it is the responsibility of The Company to store it in a secure environment.
- In the event of information security breach, The Company shall be in a position to demonstrate that information security is implemented as per the documented information security policies. To meet this objective, appropriate record of the implementation of Information Security controls should be maintained in such a manner that it would be acceptable as evidence.
- If the Personal information is available in physical document form, it shall be kept in protected environment such as physical security system, cupboards, fireproof cabinets, file storing equipment and machines, etc.
- If the Personal Information is available in electronic format it shall be stored within the Company's environment and software systems, which shall be protected with the help of appropriate access controls, passwords, encryption

and/or other such reasonable security measures Personal Information of Customers shall not to be copied, duplicated, or extracted for any purpose other than for the Company's operations / legal and/or regulatory requirement.

### **Modifications to the Personal Information**

- The Company shall provide facility to Customers to review their Personal Information. In case any changes are required such as address, contact details etc., the Company shall facilitate customers to make those changes, and ensure that necessary supporting documentation is obtained from the Customers for Company's record.
- The Company shall ensure that the Customers are clearly informed that the Company shall not be responsible for the authenticity of the personal information or sensitive personal data or information supplied by the provider of information to The Company or any other person acting on its' behalf.
- Before collecting Personal Information, the Company shall ensure that the Customer is duly informed that it is purely in their interest to provide current, accurate, complete and valid Personal Information.
- A copy of Customer's Information shall be made available if requested by the Customer and the Customer is entitled to have any inaccuracies corrected.

### **Grievances / Complaints**

The Nodal Officer for Public Grievances at Head Office shall be the Grievance Officer for Data Privacy related issues, whose name and contact details shall be provided on the Company's website.

The Complaints made to such Grievance Officer shall be redressed expeditiously, as per regulatory guidelines.

### **Sharing / Transfer of Personal Information**

- In pursuance of the Policy, it shall be the responsibility of The Company not to disclose Personal Information of Customers to any third party. However, the Company may be required to share Personal Information to its Service Providers and Authorized Vendors in order to render service to Customers. In such cases, before sharing any such Personal Information, The Company shall ensure that a proper Agreement is signed by the recipient Service Providers and Authorized Vendors and they are bound by confidentiality conditions.

- The Company shall ensure that such Personal Information shall be transferred / transmitted to other body, corporate or a person in India or abroad, as required in the normal course of business, only when the other entity ensures the same or higher level of data protection is adhered to, by the Company.
- Transfer of Personal Information of customer to other entity shall only be allowed pursuant to a valid contract between the Company and such other entity which clearly states the need to transfer such Personal Information of its' Customers.
- The Company may disclose personal information to Banks, Society, Any Govt. Agency, law enforcement agencies and identity and address verification agencies, etc. who may record and use Customer Information and disclose it to other organizations for a lawful purpose or connected with a function or activity or business of the Company.

### **Permitted Disclosure**

- The Company shall take prior permission of Customers before disclosing, publishing any Personal Information provided by Customers, unless the company is required to make such disclosures under compliance of legal obligations.
- The Company, shall share Personal Information without obtaining prior consent of Customer to Government agencies mandated under the law to obtain such Information for the purpose of :
  - verification of identity or
  - prevention, detection, investigation of crimes or
  - prosecution and punishment of offences or
  - in national interest
- The Company shall disclose Personal Information of Customers, after due verification of the requirement from Government agencies, stating the purpose of seeking such Personal Information and that such information is required for some legal purpose. Moreover, the Company shall also obtain commitment that the Personal information so shared shall be used for the purpose for which it is obtained and shall not be published or shared with any other person.
- Personal Information shall be shared with a third party only as per an order received by the Company under the prevailing law. Such disclosure of Personal Information shall be done by the Company, only after receiving a commitment from the third party that it shall not make further disclosures.

- Personal information shall not be shared with third parties for the purpose of direct marketing unless express consent is obtained from the Customer for the same.

### **Retrieval of Personal Information**

- The Company shall ensure that the Personal Information retrieved in physical or electronic format, is returned to the secure environment or securely destroyed after the required usage.
- In case any copy of Personal Information needs to be created for the purpose of the Company's operations, it shall be the responsibility of the Company to store the copies in a secured environment and restore such copies also to the secure environment or destroy securely.

### **Access of Personal Information**

Only the Company Employees, and employees of the Business Correspondents, Agents, Service Providers who are authorized by the Company shall be allowed to access the Personal Information; provided a lawful contract is made and their operational duty demands access to such Personal Information on a need-to-know basis.

### **Prevention of Unauthorized disclosure**

Company shall maintain the following policies and procedures to prevent unauthorized disclosure of information

- a. Policy and procedure to secure the confidentiality of the data, information
- b. Policy and procedure to ensure that access to the data, information is permitted only to such of their managers or employees or designated officers, who are duly authorized for the purpose on a need to know basis;
- c. Policy and procedure to ensure and control, access to the data, information by means of physical barriers including biometric access control and logical barriers by way of passwords;
- d. Policy and procedure to ensure that the passwords used in this behalf is not shared by anyone else than who is authorized in this behalf and the passwords are changed frequently, but on irregular intervals;

- e. Policy and procedure to ensure that the best practices in relation to the deletion and disposal of data, especially where records or discs are to be disposed of off-site or by external contractors, are followed;
- f. Policy and procedure to ensure that the system adopted for the purpose shall provide for protection against an unauthorized modification or deletion of the data, information
- g. Policy and procedure to ensure maintenance of log of all accesses to data, including the following namely:-
  - i. The identity of the person seeking access to the data
  - ii. The date and time of such access;
  - iii. The identity of the Customer whose data were so accessed; and
  - iv. The records and entries pertaining to such log is preserved for minimum period as per backup policy/electronic record management policy/guidelines and the same could be available for examination by auditors / or by the Reserve Bank / or by any other Govt. regulatory agency, as the case may be;
  - v. Policy and procedure to ensure that the records and entries pertaining to maintenance of log of all unsuccessful attempts to access data end, all incidents involving a proven or suspected breach of security in respect thereof including therein;
  - vi. The requisite particulars the records affected, if any and action taken in respect of such access;
  - vii. Procedure for security incidence reporting and response
  - viii. Maintenance and review of records and entries of log, on a regular and frequent basis to detect and investigate any unusual or irregular patterns of use of or access to data including creation of the audit trails and verification thereof;

### **Accidental / Unauthorized Disclosure**

- In case any Company Employee or Service Provider or Authorized Agent identifies that Personal Information of any Customer is erroneously disclosed in contravention of this Policy, then the entity shall immediately inform such incident through the reporting channel to the Grievance Officer.
- Depending upon the criticality of the information and its' impact, the Company shall take suitable actions in such matters.

### **Protection under Whistle Blower Policy**

If any of the Company's Employee, Agent, Service Provider, Authorized Agent, etc, observes that Personal Information of a Customer is being disclosed in contravention of this policy, such person/entity shall be encouraged to inform such incident pursuant to the Whistle Blower Policy of the Company.

### **Disposal of Personal Information**

The Company shall destroy Personal Information in its possession, when it is concluded that such information is no longer needed and the Company is not under a legal obligation to retain the information anymore. Due precaution shall be taken prior to destruction of such information.

### **ENFORCEMENT**

The Company shall have a "Chief Information Security Officer (CISO)", who shall be the CEO of the Company.

The CISO shall be responsible for articulating and enforcing this Privacy Policy, protecting the Information of the Company and also for coordinating the Personal Information security related issues/implementation within the Company as well as relevant external agencies.