Policy on Data Privacy

Contents

1. Purpose

This policy specifies the data privacy requirements shall be integrated in information security practices Pioneer Financial & Management Services Limited (hereinafter shall be referred as "Pioneer Financial"). This policy is intended to comply with any privacy regulations as applicable.

2. Scope

This policy applies to all individuals who access, use or control Pioneer Financial owned resources. This includes but is not limited to Pioneer Financial's employees and third parties (contractors, consultants and other workers including all personnel affiliated to external organizations) with access to the Pioneer Financial's resources, network. This policy is applicable for both the locations (Kolkata, Mumbai) of Pioneer Financial.

3. Roles and Responsibilities

S.No.	Key Practice	Responsibility Of
1.	Adherence to this policy	Information Security / Technology / HR teams / Admin & Travel

4. Policy Statements

4.1 Information collected by Pioneer Financial

For day-to-day functions, Pioneer Financial may collect and/or hold personal information

4.2 Personal Information

This includes information that meets the following descriptions:

- Name;
- Mailing and/or street address;
- Email address;
- Telephone number;
- Profession, occupation or job title;
- Pioneer Financial may also collect personal information from individuals seeking employment with Pioneer Financial (including contractors) relating to their suitability as an employee as well as employees of Pioneer Financial, including:
    - Age or date of birth;
    - Marital status;
    - Insurance details (relating to superannuation and pensions);
    - Banking details;
    - References from previous employers;
    - Employment suitability information obtained from recruitment agencies or related entities acting on Pioneer Financial's behalf;
    - Information from law enforcement agencies, including whether or not the individual hasa criminal record;
    - Educational or vocational organizations to the extent necessary to verify employee's qualifications.

4.3 Collection of personal information

Pioneer Financial may collect personal information:
Through access to, and use of, Pioneer Financial website; From written requests, including email;
When an employee or candidate complete an application, either online or hard copy, regarding any of the services or opportunities included in Pioneer Financial; or
Through provision of identity documents such as a driver's license, passport, ID documents for the purpose of verifying identity.
Pioneer Financial may also collect personal information from third parties, including:

- Employer;
- Government agencies or regulators;

4.4 Need for personal information

Pioneer Financial collects personal information for the following purposes:
To send communications (on request)
To update records and keep contact (and other) details up-to-date (on request) To answer enquiries and provide information
To process and respond to any complaints

4.5 Use of personal information

Personal information is used for the following purpose:
To check employees and third party vendors' identity (where there is a need to comply with a legal obligation)
To notify employees about changes to administrative functions.

4.6 Sharing of personal information

Personal information held by Pioneer Financial will only be used for purposes directly related to one or more legitimate functions or activities of Pioneer Financial in the provision of its services or as otherwise permitted by law.
Pioneer Financial may disclose personal information to:

- Employees as required in order to use information for administrative purposes
- Contractors or third parties, in order to perform identity verification
- IT systems administrators, web hosting providers, mailing houses, couriers, payment processors,

Pioneer Financial will ensure that adequate safeguards will be put in place so that personal information is held securely and in accordance with this Privacy Policy.
In some cases, Pioneer Financial may be required to disclose personal information without consent. Specific instances include where:
A warrant or notice issued by a court requires Pioneer Financial to produce records or documents held by Pioneer Financial.

4.7 Security of personal inform ation

Pioneer Financial will take all reasonable steps to ensure personal information is protected from misuse, loss and unauthorised access, modification or disclosure in accordance with statutory requirements. This includes having security measures and controls in place to protect personal information including limiting access, cryptography, physical and environmental security and audit monitoring.
Pioneer Financial may hold information in either electronic or hard copy form, and will destroy or de- identify personal information when it is no longer required or when Pioneer Financial are no longer required by law to retain it (whichever is the later).

In order to maximize the protection of data within Pioneer Financial's control, the following industry aligned best practice information security controls will be implemented:

- Information Security Management System certified to an international standard
- Firewalls on the network perimeters
- Intrusion Detection Systems (IDS) on the network perimeter
- Data Loss Prevention (DLP)
- Secure-System Development Lifecycle (s-SDLC) controlling the internal developments
- Log Management and monitoring
- Monitoring of Vendor Alerts
- Penetration Tests and Vulnerability Assessments run against the OWASP Top 10 security risks of all externally facing systems
- Anti-virus protection with regularly updated virus-definition data and
- Application of available patches through regular patching cycles.

4.8 Storage duration for personal information

Personal data will be held in Pioneer Financial systems for as long is necessary to provide services and/or perform the contract drafted during employment.

4.9 Rights of individuals

Employees have the following rights in relation to how information is used.

• Right of access – the right to know if Pioneer Financial is using individual's personal information and, if so, the right to access it.

• Right of rectification/correction – Employees have the right to require Pioneer Financial to correct any errors in the information Pioneer Financial hold about them.

• Right to erasure – in some cases, employees will have the right to require Pioneer Financial to delete their information.

5. Policy En forcement and Compliance

Compliance with this policy is mandatory and Pioneer Financial department managers shall ensure continuous compliance monitoring within their department. Compliance with the statements of this policy is a matter of periodic review.

Any breach of this policy may constitute a security violation and gives Pioneer Financial the right to conduct disciplinary and / or legal action, up to and including termination of employment or business relationship.
Disciplinary action will be dependent upon the severity of the violation which will be determined by the investigations.

6. Waiver Criteria

This policy is intended to address information security requirements. If needed, waivers shall be formally submitted to the Information Security Management & Governance Committee, including justification and benefits attributed to the waiver. The policy waiver period is for a maximum period of 4 months, and shall be reassessed and re-approved, if necessary for maximum three consecutive terms. No policy shall be provided waiver for more than three consecutive terms.

7. ISO 27001 References

- A.18.1.4 Privacy and protection of personally identifiable information

8. Document Management

Technological advances and changes in the business requirements will necessitate periodic revisions to documents. Therefore, this document may be updated to reflect changes or define new or improved requirements as and when required and annually at a minimum.
Any change will require the approval of the Information Security Management and Governance Committee (ISMGC).

9. Glossary

Term	Definition
Asset	Asset is anything that has value to the organization.
Asset Owner	Managers of organizational units that have primary responsibility for assets associated with their functional authority.
Information Security	The preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.
Policy	A plan of action to guide decisions and actions. The term may apply to government, private sector organizations and groups, and individuals. The policy process includes the identification of different alternatives, such as programs or spending priorities, and choosing among them on the basis of the impact they will have.