Policy on Information Security

Contents

1 Purpose

The Information Security Policy is aimed to assure and communicate the management commitment and intent of supporting goals and principles for information security in line with Pioneer Financial Private Limited & Pioneer Asset Management Private Limited (together hereinafter shall be referred as "Pioneer Financial") business process.

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, third parties (contractors, consultants and other workers including all personnel affiliated to external organizations), investors, customers, other internal and external stakeholders with access to the Pioneer Financial's resources, network. This policy is applicable for both the locations (Chennai, Mumbai) of Pioneer Financial.

3 Roles and Responsibilities

Each role involved in this policy shall have main responsibilities as follows:

Role	Responsibility
Information Security Management and Governance Committee (ISMGC)	• Ensuring that information security policies are compliant with Pioneer Capital legal, regulatory and contractual requirement. • Responsible for reviewing and approving policy and waivers. • Responsible for ensuring the implementation, operation, monitoring, maintenance and improvement of the Information Security Management System
Information Security Manager (ISM)	• Oversee all information security processes and serve as the focal point for all information security issues and concerns. • Developing and maintaining the information security policies, procedures, standards and guidelines. • Distributing information security documents so that those who need such documents have copies or can readily locate the documents via an intranet site. • Reviewing and periodically updating information security documents to enhance information security at Pioneer Financial. • Coordinating a response to actual or suspected breaches in the
	confidentiality, integrity or availability of critical business information. • Coordinating with the all Pioneer Financial Departments to ensure that security measures are implemented to meet Pioneer Financial security requirements. • Managing security training and awareness programs. • Conducting and managing risk management activities

Information Security Team	Ensuring the protection of information / infrastructure systems, according to the technological mechanisms defined by the system / application design team. • Maintaining the information security policies implementation and compliance within the departments. • Performing system/application/network security monitoring. • Administering critical security infrastructures (e.g. antivirus infrastructure). • Designing and implementing network and system security. • Implementing appropriate controls to protect the confidentiality, integrity and authenticity of sensitive information.
Departments	• Ensuring the protection of information / infrastructure systems, according to the technological mechanisms defined by the system / application design team. • Coordinating and maintaining the information security policies implementation and compliance within their departments. • Performing system/application/network security monitoring. • Administering critical security infrastructures (e.g. antivirus infrastructure). • Designing and implementing network and system security. • Implementing appropriate controls to protect the confidentiality, integrity and authenticity of sensitive information.
Human Resources Department	• Communicate the policies to all new employees and ensure that they understand the requirements and responsibilities towards Information Security policies. • Provide the expert legal advice that is necessary for other departments to provide services in a manner that is fully compliant with existing laws and regulations.
Information Users (Users / Pioneer Financial Employees / Contractors / Vendors / Consultants)	• Must conform to this Pioneer Financial security policy • Must inform IT staff of exceptions to this policy • Reporting actual or suspected security incidents to Help Desk. • Using the information only for the purpose intended by Pioneer Capital. • Accepting accountability for all activities associated with the use of information access privileges.

4 **Policy Statements**

1. Approach to Information Security

Information Security Policy

- Pioneer Financial is committed to preserving the security of all assets (including information) owned by and entrusted to it and ensuring the Security and Legal conformity. Pioneer Financial Management understands their responsibilities toward sustaining the information security objectives within the environment.
- Pioneer Financial Management acknowledges the importance of ensuring information security and is committed towards supporting the information security goals and its principles.
- Pioneer Financial Management shall establish information security objectives aligned to its business objectives, information security requirements and pertaining risks.
- Pioneer Financial Management shall develop detailed plans to measure, communicate, update and achieve information security objectives.
- Pioneer Financial approach to Information Security Management shall be based on internal standards and globally accepted best practices to ensure:
- Information shall only be accessed by authorized individuals, who have the proper and approved access authorization.
- All confidential information shall be well protected with all the necessary controls.
- Information shall only be changed and/or updated only by authorized individuals who have the proper and approved authorization.
- Information shall always be available to all individuals who have the proper and approved authorization to access this information.
- All Individuals who have been granted any form of access to information are fully accountable for the proper use of this information.
- Pioneer Financial shall meet all applicable legal and/or regulatory requirements pertaining to information management.
- Information Security User Awareness programs shall be conducted to keep employees informed on their security roles and responsibilities.
- Information incidents shall be reported and managed in a timelymanner.
- Business continuity and incident response plans for information services shall be maintained and tested on a regular basis.
- Pioneer Financial shall ensure continuous improvement in information security process through regular reviews and continuous management support.
- Adequate security policies and procedures shall be developed and implemented to meet the Information Security objectives.
- Management shall support the implementation of Information Security Management System to comply with ISO27001:2013 standard.

2. Commitment to Information Security

- Pioneer Financial Management shall define a well-structured Information Security Framework to initiate, control and maintain information security in accordance with business requirements. Management shall provide the direction and support for implementation of security requirements Information Security Policy across Pioneer Financial.

- Pioneer Financial Management and staff are committed to strict adherence to its information security policies and practices. All management and staff

personnel are required to comply with relevant Security Policies, Procedures and Standards.

3. Information Security Policy Review and Evaluation

    1 Information security policies, procedures and standards shall be reviewed on an annual basis as well as on need basis and updated accordingly by the Information Security team.
    2 The effectiveness of the implemented controls shall be annually measured by the Information Security team to avoid security incidents and reduce resulting impacts, together with a process for benchmarking security maturity with other similar establishments. The below shall be considered:
        1 Feedback and opinions of interested users.
        2 Reports and status of incidents reported.
        3 Results of independent and management reviews.
        4 Trends of threats and its vulnerabilities.
        5 Consult and involve human resource and legal department.
    3 Information Security Team shall ensure that its internal information security policies, and relevant procedures and standards are documented in line with relevant international standards, legal and regulatory requirements and other compliance requirements.
    4 Information Security Team shall coordinate the goals, objectives and activities of the information security management.
    5 All departments shall cooperate within themselves and with the Information Security team to ensure appropriate security level for their information assets.

5 Policy Enforcement 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 periodicreview.

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.

Information Security Policy

The policy waiver period have 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. 5.1.1 Policies for Information Security
- A. 5.1.2 Review of the Policies for Information Security
- Clause 5.1 Leadership and commitment
- Clause 5.2 Policy

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
Accountability	A security principle indicating that individuals must be able to be identified and are to be held responsible for their actions.
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.
Availability	The property of being accessible and usable upon demand by an authorized entity.
Confidentiality	The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
Control	It is a means of managing risk, including policies, procedures, guidelines, etc., which can be of administrative, technical, management, or legal nature.
Incident	A vulnerability and threat together result in an incident. An information security incident is indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.
Information Processing Facilities	Any information processing system, service or infrastructure, or the physical locations housing them.
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.
Information Security Event	An information security event is an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant.

ISMS	An Information Security Management System is a set of policies concerned with information security management.
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.
Risk	Risk is combination of the probability of an event and its consequence.
Risk Analysis	A systematic use of information to identify sources and to estimate risk.
Risk Assessment	Risk Assessment is defined as the overall process of risk analysis and risk evaluation, where risk analysis is defined as the systematic approach to identify an organization's exposure to uncertainty and to estimate the risk. Risk evaluation is the process of comparing the estimated risk against given risk criteria to determine the significance of risk.
Risk Evaluation	Process of comparing the estimated risk against given risk criteria to determine the significance of the risk.
Risk Management	Coordinated activities to direct and control an organization with regard to risk. NOTE: Risk management typically includes risk assessment, risk treatment, risk acceptance and risk communication.
Risk Treatment	Process of selection and implementation of measures to modify risk.
Third Party	That person or body that is recognized as being independent of the parties involved, as concerns the issue in question.
Threat Vulnerability	A threat has the potential to cause an unwanted incident which may result in harm to a system. Vulnerability is defined as a weakness associated with an asset.