Sonata Finance Private Limited

Information Technology (IT) Policy

Ver 1.1

Classification: *Internal use*

Prepared by:	*Megha Goel, Head Planning and Monitoring*
Reviewed by	*Anup Singh, MD & CEO Sonata Finance*
Approved by	*Anal Jain, Chairman IT Strategy Committee*

Version History

Sl No	Description of change	Version number	Date
1	First release	1.0	2nd April 2018
2	Second release based on reviews	1.1	16th April 2018

Table of Contents

Introduction:

Information Technology has become the backbone of organizations and moved from a support function to that of strategic importance. Considering the criticality of Information Technology(IT) and Information systems (IS) in SFPL, it is imperative that all IT/IS activities be established and implemented based on approved IT policies as articulated and approved by the Board of SFPL.

Note:

1. The following usages of IT and IS within this document and across other documentation within the organization are intended to mean the same.

Purpose:

In keeping with the business needs of SFPL, the following IT policiesare adopted to provide guidance to all IT efforts in the organization. This will ensure that IT continues to meet the needs of the business users, the organization and other stakeholders.

IT policy

This document captures the IT policy applicable to the organization and is described under the following heads.

1. IT Governance
2. IT Organization Structure
3. IT Risk Management
4. IT Operations Management
5. IT Change Management
6. IT Outsourcing
7. BCP
8. IS Audits

Policy statements

1. IT governance

1.1. An IT StrategyCommitteeshall be established forproperimplementationandmonitoringtheITpolicies.

1.2. Themembersofthecommitteeshallbeformedfromvariousstakeholders

1.3. Roles and responsibilities shall be defined for thoseforming part of the IT governance structure.

1.4. An IT steering committee shall be established with suitable interfaces to theManagement, IT,IT StrategyCommitteeand the Board.ThemembersoftheITsteeringcommitteeshallbeformedwithCEO/MDas Chairman,HODsandasmembers.HeadofITshallbetheMemberSecretaryandisr esponsibleforcoordinationandimplementationofactions.Externalconsultant/ smaybeco-optedtotheSteeringCommitteeasrequired.

1.5.

1.5.1. A Chief Information Officer(CIO) and Chief Information Security Officer (CISO) shall be designated/appointed..

1.5.2. The IT steering committee shall meet at least once every quarter.

1.5.3. Minutes of meetings of the steering commitment shall be kept

1.5.4. The Steering committee shall have oversight of IT operations and project/strategic initiatives.

1.6. IT strategy shall be articulated to guide IT investments and upgradations.

1.6.1. An IT strategy document shall be prepared by the IT Department and presented to the IT steering committee

1.6.2. The IT steering committee shall be responsible to vet the strategy and present it to the Board.

1.7. Actions shall be takeninsuchaway to ensure value delivery, IT risk

management, IT resource management and IT performance management.

1.7.1. IT shall report on the status of IT strategy implementation

1.7.2. Key Performance Indicators (KPIs) shall be established and reported for Business as Usual(BAU) and Strategy/Project linked actions.

1.7.3. IT shall publish a monthly dash board with information on KPI's

1.7.4. Key Risk Indicators (KRIs) shallbe established, monitored and performance reported.

1.7.5. Annual Capacity planning exercises shall be carried out for all IT resourcesincludingITinfrastructure,people,etc.

1.7.6. IT resource availability shall be monitored and managed.

1.7.7. Status of outsourced activities shall be monitored and performance reported

1.8. As part of the governance,evaluation of compliance to requirements, including but not limited to, statutory/regulatory requirements, shall be carried out at least annuallyand as necessary, and reported to IT strategy Committee and the Board.

1.8.1.

2. IT organization structure

2.1. An IT organization structure shall be established to enable the delivery of IT services as required by the organization.

2.1.1. An IT organization chart shall be prepared and staffed with competent personnel.

2.1.2. Roles and responsibilities shall be defined, assigned and communicated.

2.2. IT function shall be staffed with personnel having competencies including those needed for ensuring information and cyber security.

2.2.1. Staff competencies requiredfortheITfunctionshall be defined and documented.

2.2.2. Competencymappingshall be carried outwiththatofexisting staff andforthoserequiredinthefuture.

2.3. Steps shall be taken to ensure and maintain IT staff related skills and competencies.

2.3.1. Annual review of IT staff competencies shall be carried out in relation to the defined requirements.

2.3.2. Based on the review of the competency, actions shall be taken to provide training, upgrade skills, obtain certification or take other actions including findings skilled staff from outside the organization.

2.4. Training and awareness shall be initiated to ensure continuing upgrading of competencies for all IT staff.

2.4.1. Training shall be provided as per an annually defined plan.

2.4.2. Effectiveness of training provided shall be evaluated and records shall be maintained.

3. IT Risk management

3.1. IT risk assessment shall be carried out and actions taken to mitigate risks.

3.1.1. IT services shall be listed.
3.1.2. Risks shall be identified based on the threats and vulnerabilities considered relevant to the IT service being provided.
3.1.3. Risks identified shall be prioritized to ensure that actions can be taken.
3.1.4. Mitigation actions shall be identified for prioritized risks so that actions can be taken.

3.2. Mitigation actions shall be planned and tracked to closure.
3.2.1. Responsibilities for mitigation actions shall be assigned to specific departments/individuals.
3.2.2. Target dates will be assigned for completion of mitigation actions.
3.2.3. Status of mitigation actions shall be tracked to closure.

3.3. Risk assessment shall be reviewed at least annually or as and when changes are made which may impact the over all IT risk profile.
3.3.1. Risk assessment shall be reviewed on an annual basis.
3.3.2. Updates to risk assessment shall be carried out when changes occur in IT services, IT assets, threats, vulnerabilities, based on events/incidents etc.
3.3.3. IT risk assessmentshallbe reviewed as part of the internal audit in the organization to ensure that risk assessment is current and up to date.

3.4. Status of risk assessment shall be presented to the Board and relevant levels of management within in the organization.

4. IT operations management

4.1. IT operations shall be managed so as to support processing and storage of information, such that the required information is available in a timely, reliable, secure and resilient manner.
4.1.1. Policies and procedures shall be defined to support IT operations while ensuring consistency and continuity of operations.

4.2. IT operations shall be carried out in consideration of the applicable risks and relevant IT and other policies as approved by the Board.
4.2.1. IT operations related policies and procedures shall be reviewed and updated based on the outcomes of the risk management activities.

4.3. IT operations shall also take into consideration applicable information security and cyber security risks.
4.3.1. Cyber security risks shall be identified and assessed and actions shall be implemented.
4.3.2. Cyber security risks shall be monitored and actions shall be taken when events/incidents occur.

4.4. Acquisition of new IT systems and applications shall be carried out in line with defined policies and within the over all IT strategy as defined in the organization. At all times, actions shall ensure value delivery, risk management, resource management and performance optimization.
4.4.1. IT procurement shall be governed by Board approved procurement policy
4.4.2. Third parties shall be governed by agreements which shall be

monitored periodically and actions shall be taken.

4.5. IT operations shall be carried out considering best practices relating to design, development, testing and implementation.

4.6. Changes to IT operations shall be carried out within the purview of Board approved Change Management policy and related procedures.

5. IT change management

5.1. Change management shall be carried out in line with Board approved change management policies and underlying procedures.

5.2. Changes shall be carried out considering the risks and impacts of such changes; steps shall be taken to manage/mitigate risks and the impacts of changes. Refer to board approved change management policy.

6. IT outsourcing

6.1. IT services outsourcing shall be carried out under the purview of a Board approved policy while ensuring that outsourcing is in line with the overall strategic plan and corporate objectives. Refer IT outsourcing policy

7. IT/IS audits

7.1. IS audits shall be carried out under the purview of the Board approved IT/IS audit policy. Refer IS/IT audit policy for details

8. BCP/DR

8.1. IT BCP shall be established based on Board approved policies. Refer BCP policy for details.

9. Documented operating procedures

9.1. Documented operating procedures shall be established to implement the requirements of this policy as required.

9.2. Established documented operating procedures shall be reviewed and updated at least once annually or as and when changes are made to applicable requirements/based on risk assessments/new additions/updates to IT/IS systems in the organization/ based on information security/ cyber security incidents/ changes in statutory and regulatory requirements etc.

Implementation

1. This Board approved IT Policy shall be implemented within SFPL by relevant teams and departments.
2. Compliance to this policy and implementation status shall be evaluated at least annually in keeping with assurance requirements indicated above and reported to the Board.