Sonata Finance Private Limited

Cyber Security Policy

Ver 1.0

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	16th April 2018

Table of Contents

Introduction:

Cyberspace is defined as a complex environment consisting of interactions between people, software services supported by worldwide distribution of information and communications technology or in simpler terms Internet[1]. Cybersecurity aims at protecting company information and infrastructure from cyberattacks.

In reality cyber security has come to encompass domains such as **communications security, operations security, physical security** within the overall purview of information security and broadly refers to all security aspects relevant to the 'digital world' today often focusing on the basic tenets of confidentiality, integrity, availability and authenticity.

Further for the purposes of this document and for effective definition of the cyber security policy in the organization, reference is also made to the definition of cyber security as provided by International Telecommunication Union (ITU), which defines cyber security as the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets.

Considering the extensive use of digital technology/cyber technology in the organization, it is important to put in place a cyber-security policy.

Purpose:

The following fundamental principles guide our cyber security policy and implementation of necessary cyber security related controls:

a) Recognition of the strategic importance of cyber security.
b) Establishing appropriate governance for cyber security.
c) Importance of assigning responsibility for cyber security measures;
d) Taking a risk-based approach to cyber security so as to ensure needs of all stakeholders is met.
e) Ensuring appropriate mechanisms to detect, respond, recover and contain cyber security incidents.
f) Continual reassessment of the cyber security profile of the organization so that necessary corrective and preventive actions can be initiated as required.

[1] Cybersecurity as defined in National Cyber Security Policy of India, drafted in 2013.

Cyber security policy

Policy statements

1. **Risk assessment**
   1.1. Cyber security risk assessment shall be carried out in conjunction with IT risk assessment to ensure that relevant threats are identified and controls implemented for mitigation.
   1.2. Status of identified cyber security risks shall be monitored on an on-going basis and adjustments carried out to ensure that risk assessment is current.
   1.3. Status of identified mitigation actions shall be tracked to closure and reported to relevant levels of management.
2. **New technology adoption**
   2.1. New technology adoption will be driven by a clear understanding of the need for such technology and evaluating the fit of such technology in line with the overall IT strategy established by the organization. Consideration shall also be given to the cyber risks from such technology and the ability to mitigate such risks.
   2.2. All new technology adoption shall be reviewed in line with organizational policies and procedures and presented to the relevant level of management and / Board committees as required.
3. **Communication technology**
   3.1. Communication technology forming or supporting cyber activities in the organization shall be governed keeping in consideration risks and relevant regulatory compliance obligations.
4. **Network protection**
   4.1. The network is the key element of cyber space and suitable protection shall be ensured for all the network elements for cyber security. Suitable technologies and technology solutions including but not limited to firewalls, end-point protection, IDS, IPS etc. will be used to secure the network.
   4.2. Appropriate monitoring of network and network security shall be carried out.
5. **Information access control**
   5.1. Access to information in the organization especially in the digital/cyber medium will be controlled and provided based on an assessment of the requirements for confidentiality, integrity and availability of such information.

6. Access to computing resources

6.1. Access to computing / cyber resources shall be on a need basis.

6.2. Rights shall be assigned considering the need for segregation of duties and to prevent fraud, collusion etc.

6.3. Access rights shall be periodically reviewed and revoked / removed in case found in excess of need.

6.4. Access rights shall be removed at the time of exit / transfer or change in role.

7. Back-up & restoration testing

7.1. Back-ups of data / information shall be taken as per established policy and procedures.

7.2. Restoration shall be carried out and records maintained.

7.3. Back-ups shall be retained as per defined policy and procedures and accessibility to back-ups shall be ensured at all times.

8. Management of outsourced activities.

8.1. Outsourcing activities carried out relating to cyber/digital resources used by the organization shall be based on appropriate due diligence and evaluation of the need to outsource in line with the organization strategy and consideration of risks from any contractual arrangements and regulatory compliance obligations.

8.2. Outsourced activities shall be managed as per established policies and procedures.

8.3. Outsourced activities shall be monitored and right to audit by the organization and its stakeholders including statutory and regulatory agencies shall be ensured contractually.

9. Training/awareness

9.1. Training and awareness shall be planned and provided to relevant personnel to ensure cyber security.

9.2. Competency requirements for personnel shall be identified relating to cyber security and shall be ensured at all times.

9.3. Effectiveness of cyber security training and awareness measures shall be evaluated and necessary actions taken.

9.4. Evidence to demonstrate the delivery of training / awareness relating to cyber security shall be retained.

10. Vulnerability management

10.1. Vulnerabilities relating to the digital / cyber infrastructure shall be managed to prevent / mitigate cyber risks and incidents by carrying out periodic vulnerability assessments

10.2. Vulnerability assessments shall be carried out at least on an annual basis.

10.3. Vulnerabilities shall be identified based on an established vulnerability

management strategy.

10.4. Action plans shall be defined to remedy identified vulnerabilities and tracked to closure.

10.5. Status of vulnerability management activities shall be monitored and reported to the concerned level of management.

11. Resilience

11.1. Resilience of cyber infrastructure shall be planned and implemented.

11.2. Capability of infrastructure to meet resilience requirements on an on-going basis shall be evaluated and tested periodically and necessary actions taken.

11.3. Resilience requirements shall be considered when new cyber infrastructure is being established and shall be implemented accordingly.

12. Cyber security preparedness indicators

12.1. Cyber security preparedness shall be monitored proactively by establishing metrics.

12.2. Early warning indicators shall be identified and monitored to ensure cyber security preparedness.

12.3. Cyber security preparedness indicators shall be used for comprehensive testing through independent compliance checks and audits / for assurance programs.

13. Cyber crisis management plan

13.1. A cyber crisis management plan shall be established addressing detection, response, recovery and containment.

13.2. Cyber crisis management plan shall consider scenarios identified based on a business impact analysis.

13.3. Appropriate corrective and preventive actions shall be initiated based on the identified cyber crisis scenarios.

13.4. Cyber crisis management plan shall be evaluated at least on an annual basis and updated as required.

14. Cyber security incident analysis and monitoring

14.1. Cyber security incidents shall be identified, recorded, monitored and analyzed.

14.2. Actions including corrective and preventive actions shall be taken on cyber security incidents.

14.3. Cyber security incidents shall be reported as applicable to the relevant regulatory authorities.

15. Documented operating procedures

15.1. Documented operating procedures shall be established to implement the requirements of this policy.

15.2. The implemented documented operating procedures shall be reviewed

and updated at least once annually or as and when changes are made to the requirements based on risk assessments/new additions cyber security incidents/ changes in statutory and regulatory requirements etc.

Implementation

1. This Board approved Cyber Security Policy shall be implemented within SFPL by the 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.