Sonata Finance Private Limited

Information Security Policy

Ver 1.2

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
2			

Table of Contents

Introduction:

Information has become the lifeblood of enterprises today and this is more so in the era of digital business processes. This increasing reliance on information has brought information security to the forefront and made it imperative for enterprises to focus on information security. Enhanced information security also increases effectiveness of business processes delivering benefits to the enterprise and its customers while also enabling compliance to applicable statutory and regulatory requirements.

With the increasing importance of information in enterprises, information is now being treated as an asset thus requiring all the protections extended to any enterprise asset. Very often enterprises are handling information belonging to customers, employees and other interested parties making the value of such information extremely important. Informationsecurity is defined as protecting the Confidentiality, integrity, availability and authenticity of information within the organization.

a) Confidentiality – Ensuring access to sensitive data to authorized users only.

b) Integrity – Ensuring accuracy and reliability of information by ensuring that there is no modification without authorization.

c) Availability – Ensuring that uninterrupted data is available to users when it is needed.

d) Authenticity – For information systems it is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine.

Purpose:

The purpose of this document is to define an organization wide information security policy, which would provide management direction and support for information security in accordance with business requirements and relevant laws and regulations. The following fundamental principles will also contribute to the successful establishment of an information security policy and further implementation of the Information Security Management System (ISMS):

a) Create awareness on strategic importance of information security;
b) assignment of roles and responsibilities for information security;
c) incorporating management commitment and the interests of stakeholders;
d) Conduct risk assessments for determining appropriate controls to find acceptable levels of risk;
e) information security to be incorporated as an essential element of business processes, information networks and systems;
f) active prevention and detection of information security incidents;
g) ensuring a comprehensive approach to information security management; and
h) continual reassessment of information security and making of modifications as appropriate.

Information security policy

Sonata Finance Private Limited is committed to
Implement systems and processes to protect and safeguard the Confidentiality, Integrity and Availability of all critical information and information processing facilities and assets from internal and external threats ensuring secure delivery of micro-financing services in the interest of all our stakeholders.
We shall achieve this by:

- Establishing risk assessment criteria and processes, objectives &metrics(Key risk indicators) for implementing an effective information security management system.
- Assessing and continually improving the effectiveness of the information security management system.
- Investigating and initiating appropriate corrective actions on all information security incidents that are reported.
- Communicating information security requirements to all employees, third parties and other interested stakeholders.
- Ensuring compliance with applicable legal, statutory, regulatory and contractual requirements relating to information security.

Policy statements

Risk assessment

1. Procedures shall be established for carrying out risk assessments considering the confidentiality, integrity and availability requirements for information assets.
2. Supply chain related risks shall be suitably identified and assessed by the organization.
3. Risk assessments shall be reviewed at least once annually and updated as required.
4. Risks shall be prioritized based on management approved criteria and controls shall be implemented.
5. Responsibility and target dates shall be assigned for controls planned to be implemented and progress tracked.
6. Residual risks approval shall be obtained from the management.
7. Risks shall be updated when there are changes in processes, IT infrastructure, nature of activities etc. The procedure details triggers on when risks needs to be updated.

Objectives & metrics (Key risk indicators)

1. Key risk Indicators (KRI's) shall be established to enable tracking of information security performance.
2. Where necessary objectives i.e. specific targets and plan to achieve these targets shall be established and tracked to closure.
3. KRI will be monitored on an on-going basis and reported to IT management on a monthly basis.
4. A quarterly report will be submitted to Top management.

Organization of information security

1. An information security organization structure shall be established headed by a Chief Information Security officer (CISO).
2. The CISO shall be supported by a cross functional team established to implement information security in their respective functions.
3. The CISO shall maintain with external agencies and special interest groups as required to ensure that information security related updates are available.

Mobile devices and teleworking

1. Mobile devices used within the organization for business purposes shall be governed by a policy.
2. IT department shall apply controls to protect organization and customer information on mobile devices suitably.
3. End point protection and mobile device management(MDM) tools shall be implemented.
4. Employees shall be required to use log-in password for all mobile devices and remote wipe shall be enabled for all such devices.
5. Teleworking shall be allowed only as per organization policies.
6. Employee shall not be allowed to connect their own devices to the organization's network.
7. Email and organization business application installation on mobile devices shall be controlled and IT department shall maintain a list of employees who are authorized to use these on their devices.

Human resources security

1. Background verification checks shall be carried out prior to employment
2. All employees will be required to sign contracts that include terms and conditions relating to information security.
3. Confidentiality and non-disclosure agreement/clauses shall be included in the contracts or appointment letters as the case may be.
4. Roles and responsibilities shall be defined and communicatedthrough out the organization.
5. All employees and third party personnel working on behalf of the organization shall be provided information security training.

6. Disciplinary procedures shall be established and communicated toall employees.
7. Access rights shall be removed when employees leave the organization or are transferred.
8. Employees shall be made aware of the terms and conditions of employment including the confidentiality, which will remain valid even after they leave the organization.

Asset management

1. An inventory of assets shall be prepared and maintained including clear identification of owner of these assets
2. Policies shall be defined for the acceptable use of assets.
3. Processes shall be defined for the return of assets upon resignation, termination of employment, or transfer as the case may be

Information classification

4. Information shall be classified into 'Confidential', Internal use' and 'Public' and labeled as per defined policies
5. Procedures shall be established for the handling of assets as per applicable classification.

Media handling

1. Removable media shall be protected as per defined procedures.
2. Employees access to removable media shall be controlled and access shall be provided only on a need basis.
3. Media shall be disposed off securelyas per defined procedureswhen no longer required .Eg. (paper by shredding and electronic media by degaussing etc.)
4. Media containing information shall be protected by suitable means against unauthorizedaccess, misuse or corruption during transportation.

Access control

1. An access control policy shall be established, documented and reviewed based on business and information security requirements.
2. Users shall be provided access to network and network services only as per need and based on appropriate authorization.
3. Formal procedures shall be established for user registration and de-registration
4. User access provision and removal shall be as per defined procedures.
5. The allocation and use of privileged access rights shall berestricted and controlled.
6. Procedures shall be established and implemented to assign, manage and revoke passwords and other secret authentication information
7. User access rights shall be reviewed at least once in six (6) months as per defined procedures.

8. Access rights of employees and third party users toinformation and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon any change.
9. Users shall be required to follow organizational procedures for use of passwords and other secret authentication information.
10. Complex passwords and their changes shall be governed and controlled by the password policy.
11. Access to business applications shall be controlled as per the access control policy.
12. Employees shall not be allowed access to privileged utility programs such as "regedit' or other programs which allow override of application controls.

Physical and environmental security

1. Physical entry controls shall be established to ensure that only authorized personnel enter the organization
2. Equipment shall be placed in the organization in such a way whichprovides protection against man-made and natural threats.
3. UPS and other back-up power supply sources shall be provided as needed.
4. Equipment shall be correctly maintained to ensure its continued availability and integrity
5. Procedures shall be established to ensure that equipment or software is taken off premises only with management's authorization
6. All equipment with storage media such as laptops, desktops, severs etc. shall be handled to ensure that any media is not taken outside the organization without approval.
7. Disposal of media shall be carried out to ensure that data is not recoverable.
8. Users shall be provided training to ensure that unattended equipment is not left unsecured- desktops and laptops will be screen locked and physical security shall be implemented as required.
9. A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.

Operations security

1. Documented operating procedures shall be established and made available to all users
2. Change management procedures shall be established as per a change management policy and be applied to the organization, business processes, information processingfacilities and systems that affect information security.
3. Capacity planning shall be carried out for all information processing facilities and systems and a capacity plan shall be prepared and published annually.
4. Availability of information processing facilities shall be monitored and reviewed.
5. Operational software installation shall be controlled. IT department shall maintain an approved list of software that will be used in the organization and it shall be ensured that installation by users is controlled.

6. The clocks of all relevant information processing systems withinthe organization or security domain shall be synchronised to a single reference time source.
7. Test data shall be protected and it shall be ensured that live data is not provided as it is for testing purposes.

Malware protection

1. Anti virus/anti malware software shall be implemented across all organizational devices i.e. desktops, laptops, mobiles and servers.
2. Users shall be prevented from disabling anti malware software.
3. Performance of anti-malware/anti-virus software shall be monitored by IT and necessary actions shall be taken to ensure their availability at all times.

Back-up

1. IT shall be responsible for carrying out periodic back-ups.
2. IT shall prepare a schedule of back-up requirements of various desktops/laptops/server etc. in consultation with the businessusers and maintain records of back-up .
3. Back-up restoration shall be carried out at least once in a quarter and records shall be maintained.
4. Restoration failures shall be reviewed and necessary actions shall be taken to prevent such failures.
5. Back-up copies will be retained in a location that is safe and away from the main business location.

Logging and monitoring

1. Event logs recording user activities, exceptions, faults and informationsecurity events shall be maintained and regularlyreviewed.
2. Logging facilities and all log information shall be protected againsttampering and unauthorized access.
3. System administrator and system operator activities shall belogged and their activities regularly reviewed.

Audit trails

1. Audit trails shall be designed and implemented for all information systems.
2. IT department shall ensure that audit logs are not tampered with and that all access to audit trails is provided based on approvals and their records are maintained.
3. Auditors and regulatory agencies will be provided required access to audit trails as approved.

Network security

1. Networks shall be managed and controlled to protect information and information systems.

2. Access to the organization’s network (wired and wireless) and network services i.e. resources which can be accessed by users shall be controlled.
3. Network segregation shall be implemented based on risk assessments.

Information transfer

1. All information transfer to entities outside the organization shall be carried out to ensure that confidentiality, integrity, availability and authenticity of information is ensured.
2. Information involved in email, or other electronic messaging used by the organization shall be protected based on the risks perceived.
3. Confidentiality/non-disclosure agreements shall be used to protect the information transferred.

Effectiveness management

1. Effectiveness of the information security management system shall be monitored using KRI’s and other methods such as audit findings, management reviews etc.
2. Based on the outcomes of the analysis of above data, actions shall be taken to improve effectiveness.
3. Effectiveness of the information security management shall be reviewed as part of internal audits and also during reviews by the appropriate levels of management and status provided to the board as appropriate.

Event/Incident management

1. Procedures shall be established to ensure quick and effective response to information security incidents.
2. All personnel in the organization shall be encouraged to report information security events.
3. Events reported shall be analyzed and classified into information security based on defined procedures.
4. Responses shall be carried out as required on identified information security incidents.
5. Root cause analysis shall be carried out on information security events and incidents to identify lessons learned and take necessary actions**.**
6. Data relating to information security events and incidents shall be tracked and analyzed.
7. Procedures shall be established and responsibilities shall be allocated to ensure that event/incident information is collected, analyzed and actions taken on the root causes.
8. Lessons learned shall be identified based on the analysis of events/incidents and various policies and procedures shall be updated accordingly.

Communication and training

1. Communication about information security do’s and don’ts shall be provided to all information users within the organization irrespective of whether they are employees or contractors.
2. Information security training shall be provided to all employees and contract personnel coming in contact with information within the organization.
3. Information security training shall be provided at the time of joining the company i.e. as part of induction or other such training, and on an on-going basis including specific to job roles; refresher training shall be provided when there are any significant changes.
4. Records of training so provided shall be maintained.
5. Effectiveness of training provided shall be evaluated and actions taken as necessary.

Compliance

1. Information security requirements originating from applicable regulatory and statutory requirements and/or contractual requirements shall be identified and compliance ensured.
2. Compliance status shall be monitored periodically and reported to the relevant level of management and applicable regulatory authorities.

Implementation

1. This Board approved Information Security Policy shall be implemented within SFPL by relevant teams and departments.
2. Procedures shall be defined and responsibilities allocated to implement necessary actions for effective information security.
3. 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.