# INFORMATION SECURITY POLICY

SFPL-POL-001

**Sonata Finance Pvt. Ltd.**

**IInd Floor, CP-1, PG Tower,
Kursi Road, Vikas Nagar,
Lucknow - 226022
Uttar Pradesh, India**

## Document Control

| Document Reference Number | SFPL-POL-001 |
|---|---|
| Effective Date | 24th Apr 2022 |
| Document Owner | CIO |

## Document Ownership

| Version | Prepared by | Reviewed by | Approved By | Date Approved |
|---|---|---|---|---|
| 1.0 | CISO | CIO | ITSC | 22.09.2020 |
| 2.0 | CISO | CIO | ITSC | 29.06.2021 |
| **3.0** | CISO | CIO | ITSC | 27.05.2022 |

## REVISION HISTORY

| VERSION NO. | | RELEASE DATE | DETAILS OF CHANGES | REVIEWED BY | APPROVED BY |
|---|---|---|---|---|---|
| FROM | TO | | | | |
| 1.0 | 1.0 | 16.9.2020 | New | CIO | ITSC |
| 1.0 | 2.0 | 29.06.2021 | No changes | CIO | ITSC |
| 2.0 | 3.0 | 27.05.2022 | Addition of Vendor Management Policy | CIO | ITSC |
| 3.0 | 4.0 | 30.05.2023 | Addition of outsourcing policy | CIO | ITSC |

## Document Control Statement:

- All rights reserved and this document is confidential.
- This document is intended solely for the use of Sonata Finance Private Limited (SFPL) employees and/or the person who have executed non-disclosure agreement with SFPL.

- This document may not, in whole or in part, be copied, photocopied, reproduced, translated or reduced in any form or manner including by any electronic, digital, or mechanical means to any medium, electronic or otherwise, or machine readable form including any information storage, scanning or retrieval system without the prior express, written consent from SFPL
- If this copy is found other than the intended location(s) please inform to <Insert Mail Id Here>
- The User is advised to ensure that the appropriate version of the document is obtained for the intended use.

# Table of Contents

## Contents

## 1.0 Introduction

Information and the supporting processes, systems and networks are important business assets. Confidentiality, Integrity and Availability of information is essential to maintain competitive edge, cash flow, profitability, contractual compliance and commercial image.

Increasingly, organizations and their information systems and networks are faced with security threats from a wide range of sources, including computer-assisted fraud, espionage, sabotage, vandalism, fire or flood. Sources of damage such as computer malware, hacking and denial of service attacks have become more common, more ambitious and increasingly sophisticated. Hence, there is an immense need for every organization to have Information Security Policy which is more aligned to the business need and objective.

## 2.0 Need for Information Security

a) Dependence on information systems and services means organizations are more vulnerable to security threats. The interconnecting of public and private networks and sharing of information resources increase the difficulty of achieving access control. The trend to distributed computing has weakened the effectiveness of central, specialist control.

b) Many information systems have not been designed to be secure. The security that can be achieved through technical means is limited, and should be supported by appropriate management policies and procedures. Identifying which controls should be in place requires careful planning and attention to detail. Information security management needs, as a minimum, participation by all employees in the organization. It may also require participation from suppliers, contractors, third party employees and customers. Specialist advice from outside organizations may also be needed.

## 3.0 Purpose

The purpose of this policy is to:

a) Protect information assets of SFPL from threats, whether internal or external, deliberate or accidental.

b) Ensure SFPL's commitment to protect information, that is stored / used / created / transmitted by SFPL, from threats and maintain its integrity as a supplier of services to its internal and external customers.

## 4.0 Scope

This policy applies to all employees in all departments of SFPL, third party vendors, contractors.

## 5.0 SFPL leadership and commitment

SFPL management supports the purpose, objectives, goals and principles of information security, and is committed to implement sound security policies and procedures in protecting all information assets in its custody by satisfying all information security related requirements that are compatible with SFPL strategic business objectives.

## 6.0 Information Security Organization

To ensure effective establishment, implementation of Information Security Management System and its monitoring for continual improvement, an Information Security organization is formed within SFPL described as below.

### 6.1 Information Security Steering Committee (ISSC)

A Committee consisting of CMD, Head-Human Resources, Head-IT and Chief Information Officer (CIO) shall act as the Information Technology Steering Committee (ISSC). The CMD shall be the Chairman and CIO shall be the convener of the IT Steering Committee.

The ISSC has been established to act as a custodian and governance body of the corporate information security program by ensuring visible executive leadership, commitment and support, as well as monitor, review progress and achieve information security implementation.

ISSC on Information Security shall meet at least once in a year or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness and to review and issue necessary guidance on Information Security matters. ISSC Meeting minutes are to be recorded.

### 6.1.1 Roles & Responsibilities of ISSC

a) Periodically review the security environment & controls and recommend necessary changes in Information Security.

b) Review of Internal & external audits of Information Security and give requisite direction.

c) Approve major initiatives to enhance information security.

### 6.1.2 Chief Information Security Officer (CISO)

Senior Executive of the level of Senior Manager or above rank shall be nominated by Chairman & Managing Director (CMD) as the CISO for the Organisation.

CISO shall be the top most nodal executive responsible for all aspects of Information Security in SFPL. CISO shall be assisted by Deputy Information Security Officer/s (DISO) regarding all IT security related issues.

### 6.1.3 Role & Responsibilities of CISO

CISO shall have a broader responsibility of planning, organizing and implementing information security across the organization on the direction provided by ISSC. Responsibilities shall include,

a) Assess business drivers and carry out a threat profile on the organization

b) Perform Risk Assessment

c) Develop security architectures at an organization level, application, network and component level

d) Identify solutions at architecture level.

### 6.1.4 Local Information Security Officer (LISO)

Head of IT Section in charge of Divisional or Regional offices will be additional charge of Local Information Security Officer (LISO) for their & subordinate offices.

Local Information Security Officers shall report directly to CISO for IT Security related issues and work under his overall direction

### 6.1.5 Role & Responsibilities of LISO

LISO shall co-ordinate the implementation of the security policy and procedures under their areas of control and carry out all the jobs assigned by CISO and report the status periodically.

### 6.1.6 Special interest groups

Specialist Information security advice shall be sought from internal and / or external sources such as CERT (International as well as local), Information Systems Audit & Control Association (ISACA), industry forums, external information security consultants and other important forums.

### 6.1.7 Contacts with authorities

Necessary contacts shall be maintained or established at appropriate times with external bodies regarding security issues. SFPL shall consult with the following external bodies, as and when needed, for mutual advice and cooperation on security issues:

I. Ambulance Services
II. Police Authorities
III. Nearest hospital
IV. Electricity and water authority
V. Communication and internet bandwidth provider

### 6.2 Information Security Working Committee (ISWC)

A committee consisting of CIO, IT Head and CISO, Deputy IT Head, System Admin constitutes Information Security Working Committee ISWC.

The ISWC has been established to act as a responsible body to ensure information security is implemented in accordance with various policies, procedures, review progress and achieve information security implementation.

ISWC on Information Security shall meet at least once in a year or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness and to check, monitor and review implementation of Information Security across SFPL. ISWC Meeting minutes are to be recorded.

### 6.2.1 Roles & Responsibilities of ISWC

a) Periodically review the implementation of controls and recommend necessary changes in Information Security to ISSC.
b) Review of Internal & external audits of Information Security and ensure compliance.
c) Suggest / recommend further initiatives to enhance information security.

## 7.0 Management review

a) The policy, with its supporting guidelines and procedures will be reviewed by the ISSC and at planned intervals to ensure its continuing suitability, adequacy and effectiveness.
b) The CIO will also review and evaluate the policy in response to any changes affecting the basis of risk assessment such as infrastructure changes, technological changes, significant security incidents, new vulnerabilities, etc.

More details are available in SFPL-Info Sec-Procedures Document (Information Security Roles and Responsibilities)

## 8.0 Acceptable Usage Policy

### 8.1 Purpose

The purpose of this policy is to ensure that all users which include support personnel and management of SFPL make use of computing systems, facilities and services according to its business requirements, lawful behaviour, trust, integrity and in accordance with local laws, ethics and culture of SFPL

### 8.2 Scope

This policy applies to all employees in all departments of SFPL, third party vendors, contractors.

### 8.3 Policy Guidelines

Every user shall be responsible for the security of all information under his/her custody and the user account operated and maintained by him/her on the server.

User shall ensure that the computing resources provided by the organisation are strictly used in line with the terms of this policy and procedures established under this policy

### 8.4 Applicability

This policy is applicable to locations of SFPL that contain information processing facilities. This policy is applicable to all employees, contractors, part-time and temporary workers, service providers, visitors, and those employed by others to perform work on SFPL's premises and who have been granted access to SFPL's premises. All such personnel are referred to as users in this policy document.

### 8.5 Enforcement

a) Users shall be constantly reminded about their responsibilities through security awareness programs, awareness posters etc. Any violation of this policy by users may lead to disciplinary action, up to and including termination of employment.

b) Third Party Consultants, Entities, Contractors, Suppliers and Vendors accessing SFPL's infrastructure shall be governed by this policy to the extent it is applicable to them. The enforcement will be through non-disclosure agreement entered by them with SFPL.

## 9.0 Mobile Devices Policy

### 9.1 Introduction

Improper use of mobile devices and remote access methodologies may expose SFPL to malicious attacks, unauthorized usage of data, theft of information, damage to critical applications, loss of revenue and damage the reputation of SFPL. Mobile devices or movable information assets include all physical assets belonging to SFPL that are movable and can be carried from one place to another including laptops/notebooks or any other communication device including data cards and cameras

### 9.2 Purpose

The purpose of this policy is to define controls for usage of mobile devices within SFPL.

### 9.3 Scope

This policy applies to all staff, including contractors and interns etc. working for, or under the control of SFPL.

### 9.4 Policy Guidelines

**Visitors**

a) Mobile devices of visitors, vendors and third party personnel shall be allowed in information processing facilities of SFPL after pre-approval from IT department.
b) Department. Details of mobile devices that are allowed access into information processing facilities of SFPL shall be reviewed on monthly basis by IT department/HR

**Employees**

a) Employees shall sign acceptance and terms of use of mobile devices. Terms of use shall adequately cover user accountability, responsibility and liability.
b) Users of laptop and other mobile devices should prevent damages to the equipment due to inappropriate handling.
c) If laptop is to be left behind for the day or for the weekend, the laptop should be locked in a secure cabinet.
d) Employees shall file police report immediately on loss or theft of mobile device(s) and shall also notify Admin Manager and Sr. Manager (IT).
e) Care should be taken that laptops are not to be packed in checked in baggage while travelling. The user shall ensure that the laptop is always under his/her supervision and never left unattended.

### 9.5 Communication Matrix

| Type of Communication | Objective of Communication | Initiator | Distribution List | Approving Authority |
|---|---|---|---|---|
| Carrying personal laptops, camera, USB Pen drives etc | To seek approval/allotment for carrying personal laptop, camera, pen drives etc | Concerned User | HR or Sr. Manager (IT) | Sr. Manager IT & HR |
| Loss or theft of laptop/any mobile device | To communicate about loss/theft of laptop/mobile device | Concerned User | * FIR in Police Station<br>*HR / Admin Manager /Legal/r Sr. Manager (IT) | |

### 9.6 Applicability

This policy is applicable to locations of SFPL that contain information processing facilities. This policy is applicable to all employees, contractors, part-time and temporary workers, service providers, visitors, and those employed by others to perform work on SFPL's premises and who have been granted access to SFPL's premises. All such personnel are referred to as users in this policy document.

### 9.7 Enforcement

Users shall be constantly reminded about their responsibilities through security awareness programs, awareness posters etc. Any violation of this policy by users may lead to disciplinary action, up to and including termination of employment.

Third Party Consultants, Entities, Contractors, Suppliers and Vendors accessing SFPL's infrastructure shall be governed by this policy to the extent it is applicable to them. The enforcement will be through non-disclosure agreement entered by them with SFPL.

## 10.0 Access Control and User Management Policy

### 10.1 Introduction

To prevent an unauthorized access to information systems a formal policy shall be framed, accepted and followed by SFPL's management to control allocation of access rights to information systems and services.

Special attention shall be given, where appropriate, for initial registration of new user, final de-registration of users, allocation of privileged access rights and restrict users to override system controls.

### 10.2 Purpose

The purpose of this policy is to secure information assets, employees and information processing facilities of SFPL by defining rules for the creation, monitoring, control and removal of user access to IT assets and services based on the business requirements

### 10.3 Scope

This document sets out SFPL's arrangements for limiting the access to information and information processing facilities based on 'need to know –need to do' principle; ensuring authorised user access and to prevent unauthorised access to systems and services; making users accountable for safeguarding their authentication information; and preventing unauthorised access to systems and applications.

## 10.4 Policy Guidelines

### 10.4.1 User access provisioning

a) SFPL shall establish and implement an authorization process for all user access privileges to all systems based on job roles and nature of information handled by them. All such privilege determination process shall be documented, approved and periodically reviewed.

b) Passwords are currently the principal means of secret authentication of a user and validating their identity to access to the Information Systems and services.

c) Systems and applications that contain sensitive or confidential information shall be segregated; isolated and appropriate access controls shall be made available to prevent data leakage.

d) Revision of access privilege shall take place whenever there is a change in the organizational status of employees, including termination or transfer of users.

e) The allocation of user access privileges to information systems and services is controlled as contained in this policy and any management directive that may be issued in this regard.

f) This policy is supported by a set of formal procedures that are in place, covering all stages in the life-cycle of user access management; starting with initial registration of new users and ending with the final de-registration of users who no longer require access to information systems and services. User shall be given access to the systems / devices using an individual username and password. Username and password used by the users shall follow the (Password Management Policy).

g) At least once in six months, SFPL shall review the user access that has been granted and ensure that access privilege granted is still valid.

h) On the request of the Business Unit Head or top management, access privilege shall be temporarily suspended, modified or disconnected from the network if it appears that any applicable company policy has been violated or that a user's activity is or could be a threat to the secure operation of SFPL's networked information system.

i) In order to ensure accountability of usage, access to IT resources shall be through individual user accounts. Users are responsible for security of their system and shall take adequate measures as mentioned in (Acceptable Usage Policy) to prevent unauthorized access to their system.

j) To protect the confidentiality of data, session time out shall be enabled with the help of password protected screen savers.

### 10.4.2 Network access control

a) All network and systems devices shall be identified on the network to enable the administrator to implement controls and to ensure accountability. Access to network devices and network services shall be based on job requirements. Appropriate security measures shall be adopted to prevent unauthorized access to SFPL network from outside.

b) Sharing of folders and files within the network shall be controlled. Access to files and folders shall be given based on 'need-to-know' and 'need-to-do' basis. Users shall be authenticated over the network using unique username and password to ensure accountability.

c) Access to network devices shall be through secured means and clear text protocols shall not be used. Unnecessary services shall be disabled.

d) Appropriate segregation of networks shall be enforced using the concepts such as DMZ (Demilitarized Zone) and VLAN (Virtual Local Area Network). External connection to the network shall be protected with the help of gateway firewall and proxies. All network devices shall have appropriate connection time out and shall display suitable warning banners to provide legal protection. Proper authentication mechanism using username and password shall be used while connecting users from external network to the SFPL network and through secure means such as VPN.

e) Detailed procedures and description of controls for protection of network is given in - Systems and Network Management Procedure.

### 10.4.3 Electronic messaging and Internet access control

a) Access to corporate email account and internet shall be restricted and given to users based on business requirement and proper authorization. Access to internet shall be restricted through gateway proxy. On a quarterly basis the policies enforced on the firewall shall be reviewed and modified accordingly.

b) Corporate email IDs to third parties (such as consultants and outsourced personnel) shall be given on need basis and with approval that are clearly distinguishable from the regular corporate email IDs.

c) Guidelines for acceptable usage of internet and email are provided in the - Acceptable Usage Policy. Users accessing internet and email shall comply with the policy.

### 10.4.4 Application/Information access control

Access to applications and various modules within the applications shall be limited based on the business requirements and users shall be restricted from accessing information or application system functions which they are not authorized to access.

### 10.4.5 Administrative access control

a) The administrative access to servers, applications and network devices shall be restricted to only required number of administrators. Usage of common user IDs, default user IDs and password is strictly prohibited and adequate logging and monitoring of administrative activities shall be enabled. System documents such as network diagrams, process flow-chart are to be maintained securely and hard copies are to be kept in lock and key.

b) Review of access to administrators shall be done at least once in six months to assess if high privilege access is still required for business purpose.

c) Access to configuration ports of network devices shall be protected from unauthorized usage. Unused configuration ports shall be manually shut down. All configuration ports shall be password protected. Default user names and passwords that may exist on the network devices shall be removed.

d) System and network administrators shall use system utilities to carry out certain functions as part of their day to day operations. Appropriate controls need to be established to protect access to system utilities.

### 10.4.6 Third party access control

a) External parties (including suppliers, vendors, visitors and contractors) are prohibited to access the IT infrastructure without SFPL approval. Access shall be based on business requirement and on the principle of minimum required privileges. Approval for access shall be sought from the Sr. Manager (IT) and the following information shall be clearly stated: system, services to be accessed, duration, purpose and country. Approval is not required for demo systems that reside outside the SFPL LAN or demo systems residing within SFPL DMZ.

b) Prior to providing access, the external party shall sign a non-disclosure agreement (NDA) with SFPL addressing information security risks associated with information and technology services

c) Visitors shall not be allowed to utilize any equipment or systems unless authorized by the Sr. Manager (IT) and the owner of the system. Access to systems shall be granted only on written confirmation by the owner of the system. The confirmation should include the application system, functions to access, permitted rights and the duration. Systems of the external parties shall be connected to the network only after it is ensured that the system is secure by way of appropriate agreement/audit. If the workstation connecting to SFPL infrastructure is owned by the visitor, it should have up-to-date anti-malware software installed and running. The workstation must not be connected to SFPL network and any other network at the same time. When the stipulated time period ends, the approver should be notified and access to the systems should be revoked.

d) When access is given to external parties, their activities shall be appropriately controlled and monitored. The external parties shall be briefed on the security policies of SFPL.

## 10.5 Communication Matrix

| Type of Communication | Objective of Communication | Initiator | Distribution List | Approving Authority |
|---|---|---|---|---|
| User Access Privileges | To authorize users to access files & folders as per their job role | Reporting Manager | IT helpdesk | Reporting Manager |
| Registration of New User Account & Email Id | To create a new user account and SFPL corporate email id | HR | IT helpdesk, Reporting Manager | - |
| De-registration of user at the time of separation | To delete/deactivate an existing user account at the time of separation | HR / Reporting Manager | IT helpdesk, Reporting Manager | - |
| Corporate Email Id to third parties | To seek approval and provide corporate email id to third parties | Management Approval | | MD |
| Third party access control | To seek approval for providing access to IT infrastructure to third party | Concerned User Dept. | Sr. Manager (IT),IT Helpdesk | IT Head/CISO |

| | | | | |
|---|---|---|---|---|
| Visitor access to any of the SFPL systems / equipment | To seek approval for granting access to the visitor on SFPL systems and equipment | Concerned User Dept. | Sr. Manager (IT),IT Helpdesk | IT Head / CISO |

### 10.6 Applicability

This policy is applicable to all employees, contractors, part-time and temporary workers, service providers, and those employed by others to perform work on SFPL's premises and who have been granted access to SFPL's information or systems. All such personnel are referred to as users in this policy document. This policy is also applicable to all the IT assets and services owned or leased by SFPL.

### 10.7 Enforcement

Users shall be constantly reminded about their responsibilities through security awareness programs, awareness posters etc. Any violation of this policy by users may lead to disciplinary action, up to and including termination of employment.

Third Party Consultants, Entities, Contractors, Suppliers and Vendors accessing SFPL's infrastructure shall be governed by this policy to the extent it is applicable to them. The enforcement will be through non-disclosure agreement entered by them with SFPL.

## 11.0 Information and Asset Classification Policy

### 11.1 Introduction

Information is a valuable and important asset to SFPL. Information in any form requires protection against risks that would threaten its confidentiality, integrity and availability. Suitable information security controls shall be selected and implemented. SFPL, therefore, shall take appropriate steps towards information asset management, its classification and information media handling.

### 11.2 Purpose

This policy sets out SFPL's arrangements for ensuring that information is classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.

### 11.3 Scope

This policy sets out SFPL's arrangements for the handling of information and information assets in accordance with their classification. The classification of information assets is recorded in the Information Asset Inventory.

### 11.4 Inventory of assets

a) SFPL shall ensure that an appropriate inventory is maintained for all the IT assets. Assets shall be identified with the help of unique tags which includes all relevant details about the assets. An owner shall be identified for each asset.

b) Apart from the inventory that is maintained for IT assets, an information inventory shall be maintained which will list down critical information that is maintained by SFPL.

c) Users in SFPL shall ensure that information and information assets are used for business purposes and as per Acceptable Usage Policy. All users including contractors and third party users, at the time of their separation, shall return all assets in possession of them acquired through the duration of engagement with SFPL

## 11.5 Information classification, labeling and ownership

a) Information created by users is the exclusive property of SFPL. Based on the criticality; information shall be classified and labeled. Information classification shall be reviewed annually.

b) In order to prevent unauthorized disclosure or misuse, suitable procedures for handling and storing classified information shall be established.

c) All information shall be classified according to its sensitivity and confidentiality. The asset (data) owner shall appropriately classify the information according to the following guidelines.

I. **Restricted/Sensitive**: Information that is extremely sensitive and intended for use only by named individuals within the organization. Restricted information may not be shared with external parties unless it is in compliance with legal requirements or there is a strong business justification.

II. **Confidential**: Information that is sensitive within the organization and is intended for use only by specified groups of employees. Such information shall be shared within a specific department and access by personnel of other departments is restricted.

III. **Internal**: Non-sensitive information available for usage within SFPL. Information classified as internal is not suitable for release outside the organization.

IV. **Public**: Non-sensitive information available on public domain that can be accessed by anyone.

d) When information of various classifications is combined, the resulting collection of information or new information must be classified at the most restrictive level among the sources.

e) If any information is not specifically classified it shall be treated as '**Internal**" by default.

f) Based on the classification of the assets, the information shall be labeled. The labeling must be made available on the documents and in a visible format.

g) Detailed procedure for protecting different classification of information is given in Asset Management Procedures.

## 11.6 Personal information

a) Personally Identifiable Information (PII) collected and retained shall be kept to the minimum and only for business requirements. SFPL shall ensure that adequate controls are in place to prevent unauthorized disclosure. Users who access PII as part of their business requirement shall handle the information with utmost care to ensure confidentiality and privacy.

b) Any misuse of personal information shall be dealt with seriously leading to disciplinary proceedings against the user.

### 11.7 Management of removable media

a) Usage of removable media such as USB drives and CD ROMs shall be restricted on the SFPL PCs. These devices shall be enabled only on need based and with proper approval. Sensitive information stored on such media shall be encrypted to ensure adequate protection (done by SEPS/Group Policy) in case of loss.

b) All storage media shall be kept at a secure place and access shall be controlled. The manufacturer's specifications pertaining to safe-keep of media and environment control shall be met. Defective media like Hard disk, DVD / CD Drive, etc., which are sent for repairs or for replacement, shall be verified to ensure that it contains no information.

c) The backup media that is stored shall be labeled appropriately. The label should contain a representation of the content of the media and periodicity.

### 11.8 Physical media transfer and disposal

a) SFPL shall ensure appropriate care is taken to protect the confidentiality and integrity by preventing unauthorized disclosure of data while media is being transferred from the organization's premises to other locations. Assets that need to be transferred to another location needs to have a clear justification and appropriate authorization.

b) SFPL shall ensure that disposal of any devices or media shall not lead to data leakage. A detailed procedure for disposal of assets is given in Asset Management Procedures

### 11.9 Sharing information – Internal and external

a) Within the organization, information shall be made available only on need basis and appropriate approval shall be obtained from the business unit head as deemed necessary while information is to be shared with other departments / functional units.

b) A Non-Disclosure Agreement shall be signed with the third parties before information is shared with them. Sharing of information with external parties requires a valid justification.

c) Care shall be taken to ensure that information shared is not intercepted, copied and modified. In order to protect the interest of the organization approved disclaimer shall be included in all the e-mails that are sent from the company email account.

### 11.10 Information about SFPL

a) Information about SFPL that is made public shall have proper approval from the management. Changes to the website content, which contains information about the organization shall be controlled and carried out only after appropriate permission is obtained from the management.

b) Appropriate controls shall be in place to ensure the integrity of the data available on the website.

### 11.11 Information retention

Retention period shall be determined based on the contractual requirements. Annual review shall be conducted and the information that has crossed the retention period shall be destroyed. SFPL shall ensure that data that is retained is secured (logically and physically) and its integrity is maintained.

### 11.12 Applicability

This policy is applicable to locations of SFPL that contain information processing facilities. This policy is applicable to all employees, contractors, part-time and temporary workers, service providers, visitors, and those employed by others to perform work on SFPL's premises and who have been granted access to SFPL's premises. All such personnel are referred to as users in this policy document.

### 11.13 Enforcement

Users shall be constantly reminded about their responsibilities through security awareness programs, awareness posters etc. Any violation of this policy by users may lead to disciplinary action, up to and including termination of employment.

Third Party Consultants, Entities, Contractors, Suppliers and Vendors accessing SFPL's infrastructure shall be governed by this policy to the extent it is applicable to them. The enforcement will be through non-disclosure agreement entered by them with SFPL.

# 12.0 Change Management Policy

## 12.1 Introduction

An effective way to record, track and manage all changes to reduce the risks of possible interruptions to services and loss / reduced functionality due to changes being implemented is essential. SFPL recognizes importance of change management and associated risks and therefore has formulated this policy to address vulnerabilities and associated risks.

### 12.2 Purpose

The purpose of this policy is to establish management directions and high level objectives for change management.

### 12.3 Policy Guidelines

### 12.3.1 Request for change and change approval

a) Any request for change should have a very clear justification. The justification should include a valid business requirement.

b) The User, System / Network Administrator shall raise a request for change. The request for change shall be approved by the corresponding business unit head. Only if the changes are approved by the appropriate authority, they shall be considered for implementation.

c) Based on the type of change, timeline shall be determined for carrying out the changes. In case of emergency changes, the changes may be approved post facto.

### 12.3.2 Change analysis

a) Changes that are requested shall be analyzed prior to carrying out any modifications.

b) The parameters that shall be used for carrying out an analysis shall be as follows:

   I. **Impact of change:** Based on the impact to the overall infrastructure, changes shall be appropriately classified. Depending on the classification, changes shall be handled by the appropriate personnel from the organization.

II. **Priority of Change:** The process of prioritization is very important if there are multiple change requests. Priority of change shall be determined based on criticality. If it is an emergency change, the changes shall be carried out in a very short duration of time.

III. **Security Implication**: Before carrying out a change, the security implication of the change needs to be analyzed. The stability of the infrastructure shall be taken into consideration and all risks associated with the change shall be mitigated.

### 12.3.3 Testing changes

a) All changes shall be appropriately tested before implementation.

b) Testing changes shall be allocated to designated individuals.

c) "Segregation of duties" principle shall be followed while carrying out the testing of the changes. The individual who has made changes shall not carry out the test.

### 12.3.4 Change implementation

Before implementing changes adequate measures shall be taken including.

a) **When to make the changes:** An appropriate time shall be decided for carrying out the changes. It shall be ensured that while carrying out the changes, there is minimum disruption to the production environment.

b) **Who will make the changes:** It is also important to make sure that the roles and responsibilities of the personnel who will be carrying out the changes are clearly defined. The time and resource (in terms of people or additional software/hardware) requirements for implementing the change shall be documented.

c) **Prerequisites:** all pre-requisites, such as full backup, are required to be carried out.

d) **Rollback Plan:** A plan shall be available for restoring the system to the original state.

e) **Post Implementation Verification:** Once the change is implemented the change requestor should verify if the changes made are in accordance with the request submitted.

### 12.3.5 Change management records

a) Changes to services, IT Infrastructure shall be recorded and analyzed to identify any trends or recurring changes.

b) Change control records shall be maintained to support and document changes that have been carried out.

c) The change management record shall contain details at minimum regarding request for changes, approval by business unit head, comments of the network administrator (or) system administrator, result of the testing process, user acceptance, implementation report etc.

d) Improvements identified from the change management process shall be documented and implemented.

### 12.3.6 Applicability

The change management policy and procedures shall be applicable to all changes that are carried out in the IT infrastructure. The policy is applicable to (but not limited to) changes that include applications, servers, network devices and infrastructure design.

### 12.3.7 Enforcement

Changes shall be carried out in strict accordance to the policy and procedures. Any changes that are carried out in violation of this policy and not in line with the implemented procedure shall be dealt with seriously.

## 13.0 Antivirus Policy

### 13.1 Introduction

A virus is a piece of potentially malicious programming code that will cause some unexpected or undesirable event. A malware is an abbreviated term meaning “Malicious Software”. Both are together termed as “virus” in this policy document.

Viruses can be transmitted via e-mail or attachments, downloaded Internet files, diskettes, and CDs. Viruses are usually disguised as something else, and so their presence is not always obvious to the computer user. A virus infection can be very costly to SFPL in terms of lost data, staff productivity, and/or reputation. Therefore, one of the goals of SFPL is to provide a virus free computing network.

### 13.2 Purpose

The purpose of this policy is to provide guidelines on measures that must be taken by users of SFPL computing network to help achieve effective virus detection, prevention and recovery controls.

### 13.3 Antivirus application

a) IT Department shall ensure that any workstation (servers, desktops and laptops) that is connected to the network is installed with the company approved antivirus program.

b) A new system shall be allowed to connect to the network only after it is verified that it has adequate virus protection mechanism.

c) Antivirus agents that are installed on the client systems shall be password protected to ensure that end users cannot uninstall the agent. Similarly the end users shall not have any privileges to change any configurations or disable the agent.

d) While upgrading the systems (migrating to new operating system), it should be ensured that the antivirus agent can support the new system and provide adequate protection.

e) Adequate number of licenses to cover all systems shall be available for the antivirus application

### 13.4 Antivirus scan

a) There shall be a regular scan of all the systems. All the systems including the applicable servers shall be scanned once a week and a detailed report shall be reviewed by the IT Department. Users are prohibited to disrupt or disable scanning of their system.

b) Any system that is not turned on during the scheduled scanning time will be scanned for virus immediately when it is turned on.

### 13.5 Files and attachment scanning

a) All files that are downloaded from internet shall be automatically scanned for virus infections and shall be either quarantined or deleted as appropriate. Similarly any files copied from removable media (CDs / DVDs) shall also be scanned appropriately.

b) Any attachment that is received or downloaded shall be appropriately scanned by the antivirus application.

### 13.6 Mobile code protection

Mobile codes such as ActiveX, Java Scripts, Macros etc., shall be controlled within the organization and users are encouraged not to use such codes.

### 13.7 Antivirus updates

a) Virus signatures are to be updated on a regular basis.

b) Adequate redundancy mechanism shall be made available to ensure that virus signatures are available if the main sources for providing antivirus updates are not available.

### 13.8 Tracking new virus outbreaks

IT department shall regularly monitor for any massive outbreaks and take adequate measures such as downloading specific tools or carrying out manual procedures to clean virus infections.

### 13.9 Virus protection for PCs of Third Party users

a) PCs/Laptops of third parties shall not be connected to the internal network of SFPL by default. However, if connectivity is needed for any business requirements then such PCs/Laptops shall be thoroughly checked for the presence of virus codes before connecting it to the organization’s network.

b) It shall also be ensured that system of third party users contain an antivirus application and is up-to-date with the latest virus signature.

### 13.10 Applicability

This policy is applicable to locations of SFPL that contain information processing facilities. This policy is applicable to all employees, contractors, part-time and temporary workers, service providers, visitors, and those employed by others to perform work on SFPL’s premises and who have been granted access to SFPL’s premises. All such personnel are referred to as users in this policy document.

### 13.11 Enforcement

a) Actions that are required to be followed by the end user with respect to virus protection shall be communicated through the Acceptable Usage Policy. Users shall be constantly reminded about their responsibilities through security awareness programs, awareness posters etc.

b) It shall be ensured that all systems are protected by antivirus application. Any system that is found without appropriate antivirus shall be disconnected from the network. Any user found to spread virus infection shall be subjected to disciplinary action up to and including termination of employment.

# 14.0 Backup and Restoration Policy

## 14.1 Introduction

In order to safeguard information and computing resources from various business and environmental threats and ensure business continuity, systems and procedures shall be developed and implemented for backup of all electronic business data, related application systems and operating systems software. This shall be done on a scheduled basis and in a standardized manner across the organization.

## 14.2 Purpose

The purpose of this policy is to describe SFPL approach towards managing the information backup securely.

## 14.3 Backup requirements

a) Backup shall be taken considering the business and contractual requirements and criticality of information.

b) Data shall be retained for the period necessary to satisfy both business and contractual requirements.

c) Respective business unit head shall identify the retention period for essential business data, and shall establish any requirement for archive copies to be retained.

## 14.4 Backup frequency and scheduling

a) The frequency for taking a backup shall be determined by the business unit head in consultation with the IT Department. Backup methodology has to be selected as appropriate among full backup, incremental backup and differential backup types.

b) The backup process shall be scheduled in such a way that it does not affect the business operations. Backup shall be scheduled before and after the execution of critical points in time such as end of day, end of month, end of year. Wherever it is possible backup tasks shall be automated.

c) Selection of backup media shall take into considerations the data that is going to be stored and other factors such as shelf life, rotation etc. Ease of usage shall also be considered before the selection of the media for backup.

### 14.5 Migration of backup data

Whenever there is a change in the system environment, such as application, operating system etc., it should be ensured that the backup information retained shall be compatible with the new system environment.

### 14.6 Security of backup data

a) The backup information is as critical as the original information. Adequate security controls (both logical as well as physical) shall be enforced to ensure limited access to backup data.

b) Backup media shall be stored in a fire proof cabinet under lock and key.

c) Backup media shall be stored in an offsite location to prevent the destruction of both the main source and the backup source.

### 14.7 Backup restoration

a) On a periodic basis backups shall be restored and tested for its integrity.

b) Depending on the criticality of information, data that is required to be checked for integrity shall be selected.

c) Periodicity of testing backup is provided in Backup and Restoration procedure

### 14.8 Backup logs and registers

To provide assurance that the backup has been completed properly, logging of the backup tasks shall be enabled where possible. Manual backup process shall be logged in a backup register. The backup register shall be reviewed on a monthly basis by the Sr. Manager (IT).

### 14.9 Communication Matrix

| Type of Communication | Objective of Communication | Initiator | Distribution List | Approving Authority |
|---|---|---|---|---|
| Backup requirements for a business unit | To communicate about back up requirements of a business unit and retention period of archive copies if any | Business unit head | IT Helpdesk, Sr. Manager (IT) | IT Head / CISO |
| Backup restoration request | In case of any data theft / missing information, to request for data restoration from backup media | Concerned user | Reporting Manager, IT Helpdesk, Sr. Manager (IT) | IT Head /CISO |

### 14.10 Applicability

This policy applies to respective business unit head and IT department of SFPL. This policy also applies to all servers and network devices that are owned or leased by SFPL or used on its network and are marked for backup.

### 14.11 Enforcement

Users shall be constantly reminded about their responsibilities through security awareness programs, awareness posters etc. Any violation of this policy by users may lead to disciplinary action, up to and including termination of employment.

Third Party Consultants, Entities, Contractors, Suppliers and Vendors accessing SFPL's infrastructure shall be governed by this policy to the extent it is applicable to them. The enforcement will be through non-disclosure agreement entered by them with SFPL.

## 15.0 Operational Security & Communication Policy

### 15.1 Introduction

This policy addresses SFPL need to develop, communicate and implement formal methods and procedures for communication and operation of internal organization and related third party procedures associated with day to day administration of information security related areas in Financial Services and management of IT functions.

### 15.2 Purpose

The purpose of this policy is to define controls and documented procedures so that day to day operations are process oriented, consistent and address information security effectively and efficiently.

### 15.3 Documented operating procedures

a) The operating procedures shall be planned and documented. The jobs in production area shall be planned and scheduled properly.

b) The procedures shall contain activities associated with information processing and communication facilities such as access control procedures, back-up procedures, system and network management procedures, asset management and handling procedures etc. All business units in consultation with IT team shall frame the procedures.

c) Documented operating procedures such as user manual, technical manual, system architecture and configuration shall be maintained for applications, operating systems, databases and other relevant components as appropriate.

### 15.4 Change management

Changes to the organization, business processes, information processing facilities and systems shall be reviewed and approved to ensure that they do not compromise information security.

For more details refer to - Change Management Policy

### 15.5 Capacity management

a) New systems shall be tested for capacity, peak loading and stress testing. They shall have a specified and acceptable level of performance, and resilience, which meets or exceeds the hardware baseline as defined. The IT team is responsible for capacity planning.

b) System tuning & monitoring should be applied to ensure and, where necessary, improve the availability and efficiency of systems. Projections of future capacity requirements shall take into account current & future projected trends.

### 15.6 Malware

a) Antivirus application shall be installed on all the systems. IT team shall ensure that any workstation (servers, desktops and laptops) that is connected to the network is installed with the company approved antivirus program. A new system shall be allowed to connect to the network only after it is verified that it has adequate virus protection mechanism.

b) Mobile codes such as ActiveX, Java Scripts, Macros etc., shall be controlled within SFPL and users are encouraged not to use such codes.

c) Virus signatures are to be updated on a regular basis. Adequate redundancy mechanism shall be made available to ensure that virus signatures are available if the main sources for providing antivirus updates are not available.

d) Any files copied from removable media (CDs / DVDs) shall also be scanned appropriately.

e) Any attachment that is received or downloaded shall be appropriately scanned by the antivirus application.

For further details refer to - Anti Virus Policy

### 15.7 Information backup

Adequate back-up facilities shall be provided to ensure that all essential business information and software could be recovered following a disaster or device failure. For further details refer to - Backup Policy

### 15.8 Logging and monitoring

a) SFPL shall introduce monitoring of systems, servers and other important information processing facilities to detect unauthorized activities from internal and external network and also to ensure information systems problems are identified.

b) System monitoring shall also be used to check the effectiveness of controls adopted and to verify conformity to an access policy model.

### 15.9 Clock synchronization

a) Clock synchronization to all the clocks of backend and security systems should be enabled and should be verified periodically.

b) Domain server should be designated as the master clock and it should be periodically synchronized with known accurate time source.

c) All other system clocks have to be synchronized to the domain server clock.

### 15.10 Technical vulnerability management

a) All critical servers, network equipment, firewalls and web portal will be subjected to Vulnerability Analysis (VA) yearly. The results will be analyzed and actions will be taken to fix all identified vulnerabilities within a specific time frame. The reports and the actions taken will be submitted to the ISSC periodically.

b) Unless authorized and approved by respective business unit head / reporting manager, no user shall install software on desktop or on operational environment. Business unit head / reporting manager shall consult IT department prior to approval.

### 15.11 Information transfer

a) It is highly essential that the many modes of exchange of corporate information such as e-mails, faxes, print-outs, phone conversations, and internet are not used for intentional or unintentional disclosure of information.

b) Adequate precautionary measures have to be outlined in each of these modes to prevent information leakage. Refer:  Acceptable Usage Policy

### 15.12 Segregation of duties

a) Separating the management and execution of duties or areas of responsibility, in order to reduce opportunities for unauthorized modification or misuse of information or services shall be developed.

b) Respective business unit heads shall ensure a proper segregation of duties applicable to all areas as appropriate for their operations.

c) Whenever it is not practical to segregate, other controls such as monitoring of activities, audit trails and management supervision should be considered.

### 15.13 Applicability

This policy is applicable to locations of SFPL that contain information processing facilities. This policy is applicable to all employees, contractors, part-time and temporary workers, service providers, visitors, and those employed by others to perform work on SFPL's premises and who have been granted access to SFPL's premises.  All such personnel are referred to as users in this policy document.

### 15.14 Enforcement

a) Users shall be constantly reminded about their responsibilities through security awareness programs, awareness posters etc. Any violation of this policy by users may lead to disciplinary action, up to and including termination of employment.

b) Third Party Consultants, Entities, Contractors, Suppliers and Vendors accessing SFPL's infrastructure shall be governed by this policy to the extent it is applicable to them. The enforcement will be through non-disclosure agreement entered by them with SFPL.

# 16.0 Password Management Policy

## 16.1 Introduction

Passwords are currently the principal means of authenticating a user and validating their identity to access the IT system. The creation, allocation, change and removal of passwords should be controlled by a formal management process

## 16.2 Purpose

The purpose of this policy is to establish controls for the management of passwords in SFPL systems.

## 16.3 Accountability

a) Individual accountability is the key to securing and introducing controls over any information system that stores or processes information owned by organization. Systems that are used to process or handle classified information must ensure individual accountability as part of implementing mandatory access control procedures.

b) Attaining individual accountability requires designing and implementing strong password-based user authentication mechanisms which will uniquely identify each user who handles the classified information. The security provided by a password system depends on the passwords being kept secret at all times. A password is vulnerable to compromise whenever it is used, stored, or shared.

c) Passwords have to be memorized by the end users and under no circumstances shall be written down on any medium or shared with anyone else.

d) Users shall under no circumstance share or disclose their password to others.

## 16.4 Password storage

Stored passwords should be protected by severely restrictive access controls and by one-way, non-reversible industry grade hashing algorithm. Where the operating system or the database that is deployed does this as an internal process, such process can be relied upon provided all other associated controls are fully complied with. The administrative module of any application shall not list the password in a clear text form.

## 16.5 Privileged accounts

In order to ensure adequate controls over the privileged high-level user accounts the following policies shall be made applicable for all the production systems/devices:

a) Default administrator account shall be renamed

b) Individual named users shall be created with required administrative privileges for day-to-day routine administration functions

c) Default administrator account password shall be changed and stored in a secure location in a sealed envelope for emergency usage

d) Activities of such users shall be adequately logged and audit trails are appropriately controlled.

### 16.6 Password recovery

SFPL strictly prohibits the usage of password cracking tools to recover password. Usage of password cracking tool shall be considered as a serious violation of corporate security policy.

### 16.7 Applicability

This policy is applicable to all employees, contractors, part-time and temporary workers, service providers, and those employed by others to perform work on SFPL's premises and who have been granted access to SFPL's information or systems. All such personnel are referred to as users in this policy document. This policy is also applicable to all the IT assets and services owned or leased by SFPL.

### 16.8 Enforcement

Users shall be constantly reminded about their responsibilities through security awareness programs, awareness posters etc. Any violation of this policy by users may lead to disciplinary action, up to and including termination of employment.

Third Party Consultants, Entities, Contractors, Suppliers and Vendors accessing SFPL's infrastructure shall be governed by this policy to the extent it is applicable to them. The enforcement will be through non-disclosure agreement entered by them with SFPL

# 17.0 System Acquisition & Maintenance Policy

## 17.1 Introduction

Applications provided by partners, vendors and owned by SFPL are the lifeline of the successful running of processes of SFPL. Applications include operating systems, infrastructure business applications, off-the-shelf products, services and outsourced applications. It is essential that security is emphasized and insisted from all providers that their products are secure from attacks and failures.

## 17.2 Purpose

This policy describes SFPL approach to manage application support and maintenance activities that provide adequate controls to ensure confidentiality, integrity and availability of its products. It ensures that a well-defined methodology is adopted for maintenance of applications.

## 17.3 Vendor provided applications

a) SFPL as part of the agreement / contract with vendors shall insist or give security requirements and considerations of the products or applications. Essentially, the products should be certified for in-built security considerations. This could include controls against buffer overflow, non-existence of back doors, Trojans, covert channels, etc. The declaration or certification could either be from the customer or vendor or by an accredited third party. Also, in the contracts SFPL shall insist that only after a formalized testing methodology the product or application will be put to use.

b) Any security feature found missing that could affect the business or security of SFPL should be rectified by the third party. It is also important that provision of security patches, version change, and product enhancements concerning security shall be provided by the third party as and when required. For products that are already put to use, SFPL shall insist on a declaration from the third party that all security considerations have been taken into account and the product / application is free from security threats. Wherever applicable, the program or application source code should be requested and stored safely within the premises of SFPL.

c) The service levels and deliverables should be clearly defined, agreed and signed in the agreement. Responsibility matrix for uptime, problem reporting and resolution based on criticality should be defined.

## 17.4 Operational software

a) Control shall be provided for the implementation of software on operational systems. To minimize the risk of corruption, the following controls shall be considered by SFPL:

i) Update of operational libraries shall only be performed by the nominated persons

ii) Executable codes shall not be implemented on operational systems until evidence of successful testing and user acceptance is obtained and the corresponding program source libraries have been updated

iii) To keep track of users, an audit log shall be maintained

iv) Previous software versions shall be maintained as a contingency measure

b) Decisions to upgrade to new release shall be done after approval from the respective Business unit head. Also, the security level of the patch or new program should be verified for any problems affecting this version and then implemented.

### 17.5 Security of system files

a) Controls shall be applied for the implementation of software on operating systems.
b) Test data shall be protected and controlled.
c) Strict controls shall be maintained over access to program source libraries

### 17.6 Vendor proprietary software

a) Software that are bought and owned by SFPL shall follow certain procedures and practices. Such software includes all operating systems, office and all other proprietary software such as Adobe Acrobat, WinZip, etc. Although, security is inherently considered by the reputed vendors who sell these software, care should be taken not to exceed the license limit and ensure security patches, fixes released by the vendors are updated periodically.

b) Logs of major activities carried out in such software should be recorded, stored and backed up.

### 17.7 Protection of test data

a) Access to test data should be provided only after removing the sensitive business and personal information.

b) Users should ensure that once the objective of testing the application/data has been met, such data should be deleted from the test application system or move to a secured authorized location.

c) Test data should be segregated from operational data. The use and copying of operational data should be logged to provide an audit trail.

### 17.8 Change control

a) Any changes in operating systems, proprietary software or business applications have to follow a formal change control methodology. Introduction of new business application or operating system must be documented, tested and then implemented.
b) Change request has to be accompanied by a Change Request form along with formal approval. Version control and logs have to be maintained for all changes.
c) Care has to be taken by IT team while installing patches, service packs and other updates. When operating systems are changed, business critical applications should be reviewed and tested to ensure that there is no adverse impact on organizational operations or security.
d) Vendor proprietary software should be used without attempting any modification or changes unless authorized by the Management. If any changes are required then appropriate approval has to be taken from the Vendor and this should be initiated by IT team. Change has to be carried out by IT team and the existing version or patch has to be updated. Changes shall be tested, documented and validated before being put to use.

### 17.9 Patches, fixes and updates

a) A centralized patch management system shall be put in place by IT team to download, analyze, test various patches, fixes and updates released by the vendors and then install them in the applications.

b) Any known mal-function operationally and security-wise observed, reported in third party applications has to be reported to the concerned vendors immediately. Any new updates given by vendors have to be version-controlled to prevent attacks.

c) In case of proprietary software of vendors, patches and fixes are released by vendor periodically. IT team shall download, test and update the patches as and when deemed necessary.

### 17.10 Applicability

This policy is applicable to locations of SFPL that contain information processing facilities. This policy is applicable to all employees, contractors, part-time and temporary workers, service providers, visitors, and those employed by others to perform work on SFPL's premises and who have been granted access to SFPL's premises. All such personnel are referred to as users in this policy document.

### 17.11 Enforcement

a) Users shall be constantly reminded about their responsibilities through security awareness programs, awareness posters etc. Any violation of this policy by users may lead to disciplinary action, up to and including termination of employment.

b) Third Party Consultants, Entities, Contractors, Suppliers and Vendors accessing SFPL's infrastructure shall be governed by this policy to the extent it is applicable to them. The enforcement will be through non-disclosure agreement entered by them with SFPL

# 18.0 Compliance & Audit Policy

## 18.1 Introduction

This policy lays down the treatment intent towards compliance with contractual, legal and ethical requirements. This policy also ensures compliance of systems and personnel with organizational policies, procedures and standards.

This policy sets out SFPL's arrangements for avoiding breaches of legal, statutory, regulatory or contractual obligations related to information security and any security requirements and periodical audits towards compliance.

## 18.2 Purpose

The purpose of this policy is to ensure that SFPL employees, contractors, third party personnel and others who access information or information processing facilities remain compliant with applicable laws, Government directives, contractual obligations, policies, procedures and standards.

## 18.3 Applicable regulations

a) Contractual obligations (SFPL Customers)
b) Vendor contracts/agreements
c) SFPL Corporate directives
d) Local Laws & Government Directives

## 18.4 Adherence to Policies and procedures

a) It is the responsibility of users to adhere to policies and procedures. There shall be regular monitoring of user activities and the violation of policies and procedures shall attract disciplinary action.

b) As part of monitoring, management shall carry out periodic audit and inspection to ensure compliance. In this regard, SFPL may monitor the activities of the end user with the help of logs. To create awareness about policies and procedures SFPL shall conduct appropriate training sessions for users.

c) All emails shall have disclaimers, to protect the organization from any loss that may result from inappropriate usage of the email by the sender or the receiver.

## 18.5 Information systems audit considerations

a) Information security stand point of SFPL shall be audited periodically as per the approved audit calendar by competent personnel who are independent of the activities being audited.

b) Reasonable resources for performing audits and reviews (such as access to systems, data, technical staff, procedures, and any special processing or reports) must be identified by the auditors, agreed and made available by management.

c) Owners of the audit tools, software and associated data must ensure that they are suitably protected against unauthorized access to prevent any possible misuse or compromise.

d) Procedures related to audit is given in - Monitoring and Audit Procedure.

### 18.6 Protection of records

a) SFPL shall ensure that important records including personally identifiable information shall be protected from loss, destruction and modification. The records are to be retained according to the contractual or business requirements.

b) The retention period is decided based on the requirements and appropriate care shall be taken to protect the documents from damage and unauthorized access.

### 18.7 Adherence to agreements

a) SFPL shall ensure compliance with any agreement it has signed with other entities. Usage of third party information shall be strictly in accordance with the agreement and any applicable regulatory and legal requirements.

b) Compliance with contractual obligations signed with the suppliers shall be monitored and complied with to prevent any legal proceedings/penalties.

### 18.8 Copyright

Infringement of copyright is a criminal offence. SFPL employees should be aware of, and should comply with, the contractual provisions in this regard.

### 18.9 Software licensing legislation

Copying and distributing licensed software is illegal, unless the owner of the software expressly grants permission. The following should be considered while implementing the policy:

a) Software shall not be copied and distributed across the computer network the violation of which may lead to legal action.
b) Use of unlicensed software by contractors and consultants on SFPL premises should be prohibited, as it could result in legal action against SFPL.
c) Software licenses, paper & electronic copy, shall be kept in safe custody, and if required, shall be produced for inspection.
d) Strong internal controls should be implemented to ensure that the maximum number of permitted user licenses is not exceeded.
e) Resale of old or redundant computer equipment can result in infringement of the copyright law, as software license agreements may not be transferable; so all the software on the storage media shall be expunged.
f) Shareware / freeware software shall not be used.
g) Cracking or breaking the licenses of software is prohibited.
h) Software license contracts must be renewed on time.

### 18.10 Independent review

#### 18.10.1 Scheduled, periodic review

The control objectives, controls, policies with supporting guidelines, procedures and processes shall be independently reviewed once in a year to ensure their completeness, effectiveness and usability.

### 18.10.2 Unscheduled review

The CISO will also review control objectives, controls, policies with supporting guidelines, procedures and processes in response to any changes affecting the basis of the original risk assessment such as organizational changes, technological changes, significant security incidents, new vulnerabilities, etc.

## 18.11 Applicability

This policy applies to employees, contractors, consultants, temporaries, and other workers of SFPL, including all personnel affiliated with third parties. All these personnel are referred to as users in this policy document. This policy also applies to all equipment that is owned or leased by SFPL or used on its network.

## 18.12 Enforcement

Users shall be constantly reminded about their responsibilities through security awareness programs, awareness posters etc. Any violation of this policy by users may lead to disciplinary action, up to and including termination of employment.

Third Party Consultants, Entities, Contractors, Suppliers and Vendors accessing SFPL infrastructure shall be governed by this policy to the extent it is applicable to them. The enforcement will be through non-disclosure agreement entered by them with SFPL.

# 19.0 Incident Management

## 19.1 Introduction

In the course of providing services to its clients, SFPL may encounter an event or chain of circumstances that has an impact or may have a potential of impact on confidentiality, integrity and availability of information systems and/or information processing facilities. Occurrence of such information security incidents can be due to technology factors and / or human action / inaction. In all cases, emphasis shall be laid for a quick, planned and coordinated response that shall mitigate the impact of the incident.

Incident response shall also help SFPL to learn the causes that have caused the incident and hence aid in taking appropriate action to prevent the incident from reoccurring.

## 19.2 Purpose

The purpose of this policy is to provide an effective way to respond to information security incidents to minimize damages

## 19.3 General

a) Incident Management starts prior to the incident with preparation for managing the incident and will end when the incident is resolved and lessons learnt have been recorded and catalogued.

b) Incident management involves various stages with each stage requiring different skill sets and time frame to respond.

c) For some incidents, resolution means restoration and continuation of services affected; other Incident resolution will involve inputs and triggers to other processes like Change Management. Incidents triggered due to malicious intent may lead to initiating disciplinary proceedings.

## 19.4 Incident identification

a) Incident shall be identified by any user of information assets, who finds something unusual, suspicious, and incorrect in the functioning and behavior of Information Systems. Examples of information security incident are, but not limited to, as follows:

**i.** A user notices that existing security control that is in place is either weak or has become ineffective

**ii.** Breach of physical security controls

**iii.** A human error causing disruptions to systems or services

**iv.** Non compliance with information security policies or procedures

**v.** Malfunctioning or unusual behavior of hardware/software

## 19.5 Incident classification

a) Incidents are broadly classified into two categories:

**i.** **Incidents driven through human action / inaction**

Incidents driven through human action / inaction are those that are engineered by individuals or occur because individuals failed to adhere to designated process they must have followed. These, in turn, may trigger technology failure.

ii. **Incidents driven through technology failure**
Technology driven incidents arise from technology malfunction or wrong configuration of information assets, etc. and not because of human action / inaction.

### 19.6 Incident escalation

a) An escalation hierarchy shall be established and followed, so that suitable remedial action is triggered, as a part of the incident management process.

b) Clear responsibilities shall be assigned for those who handle different stages of an incident. In case of incidents such as intrusion or hacking attempts, if required, law enforcement authorities shall be notified.

### 19.7 Incident documentation and evidence preservation

a) A document shall be created which will include details about the incident such as how the incident occurred, the response, and whether the response was effective. This document will help in better risk mitigation and planning.

b) Appropriate evidence shall be collected against the incident. Copies of audit/system logs, email, and other communication as deemed appropriate shall be retained.

c) When tracking and responding to security incidents, any sensitive information related to the incident shall be protected and kept confidential.

d) All data related to the security incident should be preserved until the incident has been investigated and cleared.

### 19.8 Implications and closure

a) A post-incident review shall be performed. A “lessons learned” session shall be conducted so as to learn from the experience. If necessary, a set of recommendations shall be presented to the appropriate management levels to ensure that such incident does not recur.

b) As a result of the post-incident analysis, appropriate changes may be carried out to security policies, procedures, etc.

c) Depending upon the nature of these incidents, whether these incidents can be used in user awareness training, as examples of what would happen, how to respond to such incidents and how to avoid them in future, shall be considered.

### 19.9 Applicability

The incident management process shall be applicable to all incidences that threaten to affect or actually affect IT infrastructure and information security. The policy is applicable to (but not limited to) incidences that include applications, servers, network devices and infrastructure design.

### 19.10 Enforcement

Incident management shall be carried out in strict accordance to the policy and procedures. Any activities that are carried out in violation of this policy and not in line with the implemented procedure shall be dealt seriously.

## 20.0 Physical and Environmental Security

### 20.1 Introduction

SFPL recognises the importance of providing physical and environmental security for its data and information assets. The underlying complexity of the physical layout and location of the building restricts the measures that may be used to ensure only authorised access to these systems.

This policy details the physical and environmental measures necessary to protect sensitive IT systems, information and assets of SFPL. Physical and Environmental security policy also includes utilities and services supporting information processing facilities

### 20.2 Purpose

The purpose of this policy is to establish guidelines to grant, control, monitor and remove physical access and provide environmental security to information processing facilities and organizational premises in general.

SFPL will develop and deploy physical and environmental security procedures to:

- minimise losses from theft, damage or inappropriate disposal of information systems and electronic and paper held information; and
- protect its information and other assets from environmental hazards like fire, smoke, water, dust, vibration, chemical effects, electrical supply interference and electromagnetic radiation

### 20.3 Secure areas

Secure area, where mission critical or sensitive business information processes and facilities supporting them are housed, will be identified and additional access control measures will be deployed to prevent unauthorised damage, access and interference to information assets and business premises.

In addition to identifying the secure areas, additional measures will be developed and deployed to ensure minimising risks poised at following points:

- Data centre and server rooms;
- Branches, Regional offices;
- Off-site equipment and information;
- Power Supply;
- Delivery and storing area; and
- Disposal of equipment.

### 20.4 Policy Guidelines

SFPL shall ensure that appropriate controls are in place to:

a) Prevent unauthorised physical access, damage and interference to the organisation's premises and information;
b) Ensure that critical information systems are located in secure areas, protected by the defined security perimeters, with appropriate security barriers and entry controls;
c) Protect the information assets by implementing environmental controls to prevent damage from environmental threats; and
d) Regularly conduct the preventive maintenance of the utility equipment to ensure their faultless services.

### 20.5 Responsibility

Head – Administration & Premises is responsible for the implementation of controls defined in the Physical and Environmental Security Policy.

The IT and Networks functions, however, are required to support the administration function for the implementation and maintenance of physical and environmental security controls as specified in this policy.

### 20.6 Insurance

SFPL will ensure that all its critical IT assets are insured against loss due to theft or damage caused by any unanticipated events like natural calamities, fire or other incidents causing disruption to the business

### 20.7 Applicability

This policy is applicable to locations of SFPL that contain information processing facilities. This policy is applicable to all employees, contractors, part-time and temporary workers, service providers, visitors, and those employed by others to perform work on SFPL's premises and who have been granted access to SFPL's premises. All such personnel are referred to as users in this policy document.

### 20.8 Enforcement

a) Users shall be constantly reminded about their responsibilities through security awareness programs, awareness posters etc. Any violation of this policy by users may lead to disciplinary action, up to and including termination of employment.

b) Third Party Consultants, Entities, Contractors, Suppliers and Vendors accessing SFPL's infrastructure shall be governed by this policy to the extent it is applicable to them. The enforcement will be through non-disclosure agreement entered by them with SFPL

# 21.0 Cloud Computing Policy

## 21.1 Introduction

Cloud computing is an obvious option for organizations in order to have efficient and cost effective IT strategy. Cloud computing has its own unique security and compliance challenges which much be understood thoroughly before embarking on it. At the same time, cloud computing presents the opportunity to transform security practices and improve defenses. Faster development and deployment of capabilities can be addressed by IaaS, PaaS, and SaaS cloud services.

## 21.2 Purpose

The purpose of this Cloud Computing Policy is to address the utilization of cloud computing technologies, resources and related operations by SFPL by ensuring that the organization implements and maintains appropriate due diligence and sound risk management practices over cloud service provider relationships to help management verify that effective security, operations, and resiliency controls are in place and consistent with the organization’s internal standards.

## 21.3 Scope

This policy applies to all employees in all departments of SFPL, third party vendors, contractors. This policy pertains to all external cloud services, e.g. cloud-based email, document storage, Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), etc. Personal accounts are excluded.

## 21.4 Policy Guidelines

Use of cloud computing services for work purposes must be formally authorized by the ISSC. The ISSC shall ensure that necessary due diligence and risk assessment are conducted before a decision is taken to adopt Cloud Technology for performing key business processes over the cloud and while selecting a Cloud Technology provider.

While doing risk assessment, SFPL shall consider various Cloud related challenges like Vendor Lock-in, Performance, Storage, SLAs and Change Management and Compliance issues.

Compliance to ITAA 2008 Cloud Computing Provisions of the IT Act shall be ensured before enlisting Cloud services

a) For any cloud services that require users to agree to terms of service, such agreements must be reviewed and approved by the CIO, IT Head, CISO and System Admin.

b) The use of such services must comply with SFPL’s existing Information Security Policy.

c) Employees must not share log-in credentials with co-workers. The IT department shall keep a confidential document containing account information for business continuity purposes.

d) The use of such services must comply with all laws and regulations governing the handling of personally identifiable information, corporate financial data or any other data owned or collected by SFPL.

e) The CIO, CISO, IT Head, System Admin decide what data may or may not be stored in the Cloud.

f) Personal cloud services accounts may not be used for the storage, manipulation or exchange of company-related communications or company-owned data.

Pl refer to Cloud Computing Procedures for more details

### 21.5 Applicability

This policy is applicable to locations of SFPL that contain information processing facilities. This policy is applicable to all employees, contractors, part-time and temporary workers, service providers, visitors, and those employed by others to perform work on SFPL's premises and who have been granted access to SFPL's premises. All such personnel are referred to as users in this policy document.

### 21.6 Enforcement

a) Users shall be constantly reminded about their responsibilities through security awareness programs, awareness posters etc. Any violation of this policy by users may lead to disciplinary action, up to and including termination of employment.

b) Third Party Consultants, Entities, Contractors, Suppliers and Vendors accessing SFPL's infrastructure shall be governed by this policy to the extent it is applicable to them. The enforcement will be through non-disclosure agreement entered by them with SFPL

## 22.0 Vendor Management Policy

### 22.1 Introduction

The purpose of the Sonata Finance Information Security Policy is to describe the actions and behaviors required to ensure that due care is taken to avoid inappropriate risks to Sonata Finance, its business partners, and its stakeholders from any of its vendors.

### 22.2 Scope

The Sonata Finance Information Security Policy applies to any individuals that interacts, set up or manage any Sonata Finance vendors.

### 22.3 Policy

### Assessments:

- Vendors granted access to Sonata Finance **Information Resources** must sign the Sonata Finance Vendor Non-Disclosure Agreement/Business Associate Agreement.
- Vendors must be evaluated prior to the start of any service and thereafter on an annual basis.
- High-risk findings must be followed up to verify remediation.
- A vendor risk assessment must be performed on vendors with physical or logical access to confidential information or that are considered critical vendors.
- Risk assessments must be performed on all requested cloud providers before approval.
- Vendors with PCI DSS compliance requirements must have their status reviewed on an annual basis.

## Management:

- Vendor agreements and contracts must specify:
  - The Sonata Finance information the vendor should have access to,
  - How Sonata Finance information is to be protected by the vendor,
  - How Sonata Finance information is to be transferred between Sonata Finance and the vendor,
  - Acceptable methods for the return, destruction or disposal of Sonata Finance information in the vendor's possession at the end of the contract,
  - Minimum information security requirements,
  - Incident response requirements,
  - Right for Sonata Finance to audit vendor.
- If a vendor subcontracts part of the information and communication technology service providedto Sonata Finance, the vendor is required to ensure appropriate information security practices throughout the supply chain and to notify SFPL.
- The vendor must only use Sonata Finance **Information Resources** for the purpose of the business agreement.
- Work outside of defined parameters in the contract must be approved in writing by the appropriate Sonata Finance point of contact.
- Vendor performance must be reviewed annually to measure compliance to implemented contractsor SLAs. In the event of non-compliance with contracts or SLAs, regular meetings will be conducted until performance requirements are met.
- Vendor's major IT work activities must be entered into or captured in a log and available to Sonata Finance IT management upon request. Logs must include, but are not limited to, eventssuch as personnel changes, password changes, project milestones, deliverables, and arrival anddeparture times.
- Any other Sonata Finance information acquired by the vendor in the course of the contract cannot be used for the vendor's own purposes or divulged to others.
- Vendor personnel must report all security incidents directly to the appropriate Sonata Finance IT personnel within the timeframe defined in the contract.
- Sonata Finance IT will provide a technical point of contact for the vendor. The point of contactwill work with the vendor to make certain the vendor complies with these policies.
- New vendors must provide Sonata Finance a list of key personnel working on the contract.
- Vendors with logical access to information resources must provide non-repudiation authentication mechanisms.
- Vendors must provide Sonata Finance with notification of key staff changes within 24 hours of change.
- Upon departure of a vendor employee from the contract for any reason, the vendor will ensure that all sensitive information is collected and returned to Sonata Finance or destroyed within 24hours.
- Upon termination of contract, vendors must be reminded of confidentiality and non-disclosure requirements.
- Upon termination of contract or at the request of Sonata Finance, the vendor must surrender all Sonata Finance badges, access cards, equipment and supplies immediately. Equipment and/or supplies to be retained by the vendor must be documented by authorized Sonata Finance IT management.

## Waivers

Waivers from certain policy provisions may be sought following the Sonata Finance Waiver Process.

## Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

## 23.0 Data Privacy Policy

### 23.1 Introduction

This Privacy Policy describes our policies and procedures on the collection, use and disclosure of your information when you use the Service and tells you about your privacy rights and how the law protects you.

### 23.2 Objectives

We use Your Personal data to provide and improve the Service. By using the Service, you agree to the collection and use of information in accordance with this Privacy Policy.

### 23.3 Interpretations and Definitions

- Interpretation

The words of which the initial letter is capitalized have meanings defined under the following conditions. The following definitions shall have the same meaning regardless of whether they appear in singular or in plural.

- Definitions

For the purposes of this Privacy Policy:

- Account means a unique account created for you to access our Service or parts of our Service.
- Affiliate means an entity that controls, is controlled by or is under common control with a party, where "control" means ownership of 50% or more of the shares, equity interest or other securities entitled to vote for election of directors or other managing authority.
- Application means the software program provided by the Company downloaded by you on any electronic device.
- Company (referred to as either "the Company", "We", "Us" or "Our" in this policy) refers to Sonata Finance Private Limited, having its Registered Office at IInd Floor, CP-1,PG Tower, Kursi Road,Vikas Nagar, Lucknow - 226022 Uttar Pradesh.
- Country refers to: India
- Device means any device that can access the Service such as a computer, a cellphone or a digital tablet.
- Personal Data is any information that relates to an identified or identifiable individual.
- Service refers to the Sonata's products and services offered to its customers through its branch offices, website or mobile applications.

- Service Provider means any natural or legal person who processes the data on behalf of the Company. It includes any third-party companies or individuals that may be employed by the Company to facilitate the Service, to provide the Service on behalf of the Company, to perform services related to the Service or to assist the Company in analyzing how the Service is used.
- Usage Data refers to data collected automatically, either generated by the use of the Service or from the Service infrastructure itself (for example, the duration of a page visit).
- You, Your means the individual, including employee, accessing or using the Service.

## 23.4 Collecting and Using Your Personal Data

Types of Data Collected

- Personal Data

While using Our Service, we may ask You to provide us with certain personally identifiable information thatcan be used to contact or identify You. Personally identifiable information may include, but is not limited to:

- Email address
- First name and last name
- Phone number
- KYC Details
- Address, State, Province, ZIP/Postal code, City
- Usage Data

The Identity request is solely to determine who the account belongs to.

When you apply for our products or services, we collect information that is necessary to be able to properly identify you, to know your requirements, expectations, and instructions in order to provide you with those products or services. For instance, we may ask for identification information such as your name, address, date of birth, details of services etc.

Biometrics: We may use some customer biometric information with the use of your fingerprint, facial, or eye biometric information for the purpose of verifying your identity.

Each time you visit our website, we collect information about your use of the website, which may include the date and time of visits, pages visited, location information, device used and IP addresses etc.

We, including our service providers, may monitor, record electronically, and retain telephone conversations and electronic communications between you (including anyone acting on your behalf) and us. We have electronic surveillance systems like closed circuit TV and video recording of certain sensitive locations where your images may be captured.

We never ask for the information like passwords, PIN (Personal identification No.), OTP (One time passwords), card numbers, CVV / CVC and expiry date from anyone. We advise all not to share this with anyone including company officials nor keep it in any readable form.

- **Usage Data**

- Usage Data is collected automatically when using the Service.
- Usage Data may include information such as Your Device's Internet Protocol address (e.g. IP address), browser type, browser version, the pages of our Service that You visit, the time and date of Your visit, the time spent on those pages, unique device identifiers and other diagnostic data.
- When You access the Service by or through a mobile device, We may collect certain information automatically, including, but not limited to, the type of mobile device You use, Your mobile device unique ID, the IP address of Your mobile device, Your mobile operating system, the type of mobile Internet browser You use, unique device identifiers and other diagnostic data.
- We may also collect information that Your browser sends whenever You visit our Service or when You access the Service by or through a mobile device.

- **Information Collected while Using the Application**

While using Our Application, in order to provide features of Our Application, We may collect, with Your prior permission:

- Information regarding your location
- Pictures and other information from your Device's camera and photo library
- You can enable or disable access to this information at any time, through Your Device settings.
- Information regarding user location is collected from the time of login to the app.
- Data collected through access to camera and photo library is used to enable upload of documents and applications.
- The information may be uploaded to the Company's servers and/or a Service Provider's server or it may be simply stored on Your device.

## 23.5 Use of Your Personal Data

The Company may use Personal Data for the following purposes:

- to evaluate your eligibility for accounts, loans, and other products and services for which you apply
- to verify your identity in order to allow you online access to your accounts, conduct online transactions and to maintain measures aimed at preventing fraud and protecting the security of your account and personal information;
- to facilitate your transactions;

- to send you important information about your account(s), products and services;
- To provide and maintain our Service, including to monitor the usage of our Service. The informationshall be used to capture your location for the purpose of marking attendance and ensure work discipline
- To manage Your Account: To manage your registration as a user of the service. The Personal Data You provide can give You access to different functionalities of the Service that are available to You as a registered user.
- To manage and serve your loan account: To manage your loan account, recoveries and other details related to your loan account.
- To contact You: To contact You by email, telephone calls, SMS, or other equivalent forms of electronic communication, such as a mobile application's push notifications regarding updates or informative communications related to the functionalities, , including the security updates, when necessary orreasonable for their implementation.
- To respond to your enquiries and manage Your requests: To attend and manage Your requests to Us.
- • to comply with applicable law and regulation, other legal process, and law enforcement requirements; and
- For business transfers: We may use Your information to evaluate or conduct a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of Our assets, whether asa going concern or as part of bankruptcy, liquidation, or similar proceeding, in which Personal Data held by Us about our Service users is among the assets transferred.
- For other purposes: We may use Your information for other purposes, such as data analysis, identifying usage trends, and to evaluate and improve our Service, products, services, and your experience.
- We may share Your personal information in the following situations:
- With Service Providers: We may share Your personal information with Service Providers to monitorand analyze the use of our Service, to contact You.
- For business transfers: We may share or transfer Your personal information in connection with, or during negotiations of, any merger, sale of Company assets, financing, or acquisition of all or a portion of Our business to another company.
- With Affiliates: We may share Your information with any existing or future affiliates, in which case we will require those affiliates to honor this Privacy Policy.
- With business partners: We may share Your information within different departments of the company as well as with our associates or business partners.
- With Your consent: We may disclose Your personal information for any other purpose with Your consent.

## 23.6 Retention of Your Personal Data

The Company will retain Your Personal Data only for as long as is necessary for the purposes set out in this Privacy Policy. We will retain and use Your Personal Data to the extent necessary to comply with our legal obligations (for example, if we are required to retain your data to comply with applicable laws), resolve disputes, and enforce our legal agreements and policies.

The Company will also retain Usage Data for internal analysis purposes. Usage Data is generally retained for a shorter period of time, except when this data is used to strengthen the security or to improve the functionality of Our Service, or We are legally obligated to retain this data for longer time periods.

- Transfer of Your Personal Data

Your information, including Personal Data, is processed at the Company's operating offices and in any other places where the parties involved in the processing are located. It means that this information may be transferred to and maintained on computers located outside of Your state, province, country or other governmental jurisdiction where the data protection laws may differ than those from Your jurisdiction.

Your consent to this Privacy Policy followed by Your submission of such information represents Your agreement to that transfer.

The Company will take all steps reasonably necessary to ensure that Your data is treated securely and in accordance with this Privacy Policy and no transfer of Your Personal Data will take place to an organization or a country unless there are adequate controls in place including the security of Your data and other personal information.

- Disclosure of Your Personal Data

The company shares personal information with third-parties only as permitted and required by law, as per company's approved guidelines and your consent in connection with the administration, processing, and servicing of account and account-related transactions, in order to perform services for you and on your behalf.

- Business Transactions

If the Company is involved in a merger, acquisition or asset sale, Your Personal Data may be transferred. The company shall however in such case give a notice either in person or through a common circular before any Personal Data is transferred and becomes subject to a different Privacy Policy.

## 23.7 Law Enforcement

Under certain circumstances, the Company may be required to disclose Your Personal Data if required to do so by law or in response to valid requests by public authorities (e.g. a court or a government agency).

- Other legal requirements

The Company may disclose Your Personal Data in the good faith belief that such action is necessary to:

- Comply with a legal obligation
- Protect and defend the rights or property of the Company
- Prevent or investigate possible wrongdoing in connection with the Service
- Protect the personal safety of Users of the Service or the public

- Protect against legal liability

- Security of Your Personal Data

We protect information we collect about you by maintaining physical, logical, administrative, electronic, and procedural safeguards. These safeguards restrict access to your confidential information to only authorized personnel with specific need to access and utilize your information. We train our employees on how to handle your information to maintain confidentiality and privacy.

The security of Your Personal Data is important to us, but remember that no method of transmission over the Internet, or method of electronic storage is 100% secure. While We strive to use commercially acceptable means to protect Your Personal Data, we cannot guarantee its absolute security.

### 23.8 Changes to this Privacy Policy

This privacy policy is subject to change. It would be reviewed periodically, at least once in a year or upon any major changes in Acts / Rules/ guidelines/ technologies/ processes/ services/ products etc. Any changes to this policy will be effective only after approval of the Board, and when published and it will come into effect immediately.

## 24 Outsourcing Policy

### 24.1. Policy Objective

This policy addresses the assessment and management of risks associated with IT business process outsourcing. Outsourcing involves transferring responsibility for carrying out an activity (previously carried on internally) to an outsourcing provider (also known as an outsourcer) for an agreed charge. The outsourcer provides services to the customer based on a mutually agreed service level, normally defined in a formal contract. Many commercial benefits can be ascribed to outsourcing, including: reducing organizational costs, greater focus on core business by outsourcing non-core functions, access to world-class expertise and resources, and greater ability to address evolving business needs.

### 24.2. Intended audience

Senior Management of SFPL (Sonata Finance Pvt. Ltd.) responsible for the determination and selection of IT outsource vendors.

### 24.3. Policy Statement

a) Scope:

Outsourcers include: hardware and software support and maintenance staff, external IT consultants and vendors, and business process outsourcing firms.

b) Selection:

Criteria for selecting an outsourcer shall be defined and documented, taking into account the: company's reputation and history, quality of services provided to other customers, number and competence of staff and managers, financial stability of the company, quality assurance and security management standards currently followed by the company, and further security criteria defined as the result of the risk assessment.

c) Risk Assessment and Assurance:

Based on functional unit need, a suitable SFPL owner for each business function/process outsourced should be identified (this is normally a senior unit manager). The owner shall assess the risks before the function/process is outsourced, using the selection process outlined above and must consider the nature of logical and physical access to SFPL information assets and facilities required by the outsourcer to fulfill the contract, sensitivity, volume and value of any information assets involved, commercial risks such as the possibility of the outsourcer's business failing completely, or of them failing to meet agreed service levels. The SFPL shall ensure that cyber incidents are reported to the SFPL by the service provider without undue delay, so that the incident is reported by the SFPL to the RBI within 6 hours of detection. The responsibilities of the IT Function of the SFPL shall include: assisting the Senior Management in identifying, measuring, monitoring, mitigating and managing the level of IT outsourcing risk in the organisation and also ensuring that the services being provided by the service provider are as per agreed terms and conditions and meet the expectations of the business and management.

24.4. In considering or renewing an Outsourcing of IT Services arrangement,appropriate due diligence shall be performed to assess the capability of the service provider to comply with obligations in the outsourcing agreement on an ongoing basis. A risk-based approach with regards to data privacy, business continuity, cyber security, adherence to regulatory norms, necessary certifications, organization maturity shall be adopted in conducting such due diligence activities. Also, past experience and demonstrated competence to implement and support the proposed IT activity over the contract period should be assessed.

24.5. Considering their impact on existing systems and associated risks, proposals of outsourcing contracts must be presented and approved by the ITSC prior to entering into any commitments/contracts with the vendor. The ITSC will ensure that the contract is aligned to organizational strategic goals and shall decide if SFPL will benefit from outsourcing the function, taking into account the information security aspects. If the risks involved are high and the organizational benefits are marginal (e.g. if the controls necessary to manage the risks are too costly), the function shall not be outsourced.

24.6. Related risk information should be recorded in the SFPL Strategic Information System under the Risks /Strategic Risk Assessment section.

24.7. Smaller outsourcing contracts require the approval of the purchase committee. At least one of the members of committee must be CIO / IT Head.

24.8. SFPL shall ensure that their rights and obligations and those of each of their service providers are clearly defined and set out in a legally binding written agreement. Details of the activity being outsourced, including appropriate service and performance standards including for the sub-contractors, if any. The contract or agreement shall clearly define the types of information exchanged and the purpose for doing so. If the information being exchanged is sensitive, a binding confidentiality agreement shall be in place between SFPL and the service provider, whether as part of the outsource contract of a separate non – disclosure agreement. The agreement shall also clearly mention that SFPL shall be provided with effective access to all data, books, records, information, logs, alerts and business premises relevant to the outsourced activity, available with the service provider, regular monitoring and assessment of the service provider by the SFPL for continuous management of the risks holistically, so that any necessary corrective measure can be taken immediately.

Right to conduct audit of the service provider (including its sub-contractors) by the SFPL, whether by its internal or external auditors, or by agents appointed to act on its behalf, and to obtain copies of any audit or review reports and findings made about the service provider in conjunction with the services performed for the SFPL.The contract shall clearly define the parties to the contract, effective date, functions or services being provided (e.g. service levels), liabilities, limitations on use of sub-contractors and other commercial/legal matters normal to any contract.

Depending on the results of the risk assessment, various additional controls must be embedded or referenced within the contract to monitor all access to and use of SFPL facilities, networks, systems etc., and to audit the outsourcer's compliance with the contract. Following review by Procurement ensuring that Indian privileges and immunities are clearly stated, all contracts shall be submitted to SFPL Legal for final approval.

24.9. SFPL shall require their service providers to develop and establish a robust framework for documenting, maintaining and testing Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) commensurate with the nature and scope of the outsourced activity as per extant instructions issued by RBI from time to time on BCP/ DR requirements.

24.10. The Senior IT Team i.e. CIO, IT Head and System Admin of SFPL shall monitor and control its Outsourced IT activities. This shall include (as applicable to the scope of Outsourcing of IT Services) but not limited to monitoring the performance, uptime of the systems and resources, service availability, adherence to SLA requirements, incident response mechanism, etc.

SFPL shall conduct regular audits (as applicable to the scope of Outsourcing of IT Services) of service providers (including sub-contractors) with regard to the activity outsourced by it. Such audits may be conducted either by SFPL's internal auditors or external auditors appointed to act on its behalf.

************** End of Document **************