



---

# CYBER SECURITY POLICY

---

SFPL-POL-003



**Sonata Finance Pvt. Ltd.**

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

## Document Control

|                           |                            |
|---------------------------|----------------------------|
| Document Reference Number | SFPL-POL-003               |
| Effective Date            | 16 <sup>th</sup> Sept 2020 |
| Document Owner            | CIO                        |

## REVISION HISTORY

| VERSION NO. | APPROVAL/REVIW DATE | DETAILS OF CHANGES                                       | REVIEWED BY | APPROVED BY |
|-------------|---------------------|--|-------------|-------------|
| V.1         | 15-05-2018          | New  | IT Head     | ITSC/ Board |
| V.2         | 30-05-2019          | IT Updates   | CIO         | ITSC/ Board |
| V.3         | 22-09-2020          | Merger of various IT policies relating to Cyber Security | CIO         | ITSC/ Board |

## 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, digital, 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.

## INDEX

|                 |   |
|-----------------|---|
|                 |   |
| 1. INTRODUCTION | 2 |
| 2. OBJECTIVES   | 3 |

|   |    |
|---|----|
| 3. REVIEW OF CYBER SECURITY POLICY (CSP)          | 3  |
| 4. CYBER SECURITY GOVERNANCE                      | 3  |
| 5. INFORMATION SHARING & EXTERNAL RELATIONS       | 3  |
| 6. SECURE IT ARCHITECTURE                         | 4  |
| 7. CONTINUOUS SURVEILLANCE                        | 5  |
| 8. INVENTORY MANAGEMENT OF IT ASSETS              | 5  |
| 9. MAINTENANCE OF INFORMATION ASSETS              | 5  |
| 10. REMOVABLE MEDIA HANDLING                      | 6  |
| 11. NETWORK LEVEL SECURITY                        | 6  |
| 12. DATABASE LEVEL SECURITY                       | 6  |
| 13. PREVENTING EXECUTION OF UNAUTHORISED SOFTWARE | 6  |
| 14. PHYSICAL SECURITY AND ENVIRONMENTAL CONTROLS  | 7  |
| 15. SECURING CUSTOMER DATA                        | 7  |
| 16. APPLICATION SECURITY                          | 8  |
| 17. CREATING AWARENESS                            | 8  |
| 18. INTERNET ACCESS                               | 8  |
| 19. IS OUTSOURCING                                | 8  |
| 20. DATA LEAK PREVENTION                          | 9  |
| 21. ETHICAL HACKING, HONEY POT                    | 9  |
| 22. BASELINE CONTROLS                             | 9  |
| 23. CYBER CRISIS MANAGEMENT PLAN                  | 12 |
| 24. GLOSSARY                                      | 14 |
| 25. OTHER REFERENCES                              | 14 |

## 1. Introduction

To combat growing cyber threats and to enhance resilience of the Sonata Finance Pvt Ltd (hereinafter referred as SFPL) to address cyber risks, this Cyber Security Policy (hereafter referred to as CSP) is developed. CSP is a structured approach to set out the management

strategy to address cyber security concerns and the responsibilities of all personnel to prevent breaches of cyber security, and thus protect SFPL's business.

## 2. Objectives

The objectives of this policy are:

- To provide support and direction on different aspects of cyber security
- To act as a guiding factor in developing relevant guidelines, templates etc
- To create and maintain a security-conscious culture in SFPL
- To ensure compliance of legal, regulatory, and contractual requirements

## 3. Review of Cyber Security Policy (CSP)

- i. The CSP should be reviewed at least annually or whenever significant changes occur in relevant ecosystem.
- ii. Chief Information Officer (CIO) is the owner of the CSP document. The overall owner of the cyber security initiative within the SFPL is CIO.

## 4. Cyber Security Governance

- i. Cyber Security Governance Structure consists of the CIO, IT Head and CISO, Deputy IT Head, System Admin.
- ii. CIO shall also be part of the overall Cyber Security Governance Structure.
- iii. These personnel are responsible for development, implementation, operation, maintenance and continual improvement of Cyber Security.

## 5. Information Sharing & External Relations

- i. Contacts with law enforcement authorities, fire department, emergency services shall be maintained by CIO office. CIO shall put in place information sharing arrangements with CERT-In

- ii. Information Asset Owner shall ensure compliance to each of the Laws and Acts relevant to its operations. These shall include but not limited to the Information Technology (IT) Act, Intellectual Property Rights (IPR), etc.

## 6. Secure IT Architecture

Following aspects shall be integral part of SFPL’s IT Architecture:

- i. SFPL’s all critical applications including outsourced shall be hosted in Layer-3 or above data centre
- ii. Applications hosted outside Layer-3 or below Data environment shall need to be risk assessed separately and placed to IT Steering Committee (ITSC) at least once in a year
- iii. SFPL’s BCP strategy shall be based on classification of applications or process:

| Application Usage          | Example  | RPO        | RTO        | Backup Server | DR Site |
|----------------------------|----------|------------|------------|---------------|---------|
| Business Application (LMS) |          | 30 Minutes | 30 Minutes | Y             | Y       |
| Internal Collaboration     | Mail     | 24 Hours   | 4 Hours    | Y             | N       |
| Internal Data MIS          | MIS      | 24 Hours   | 12 Hours   | Y             | N       |
| Internal Financial         | Treasury | 30 Minutes | 30 Minutes | Y             | Y       |

- iv. IDS, IPS, Firewalls, Internet Gateway, Mail Gateway, DDOS protector, Application Delivery Controllers, DNS servers, Routers & Switches etc. shall have secure configuration and shall be part of continuous surveillance.
- v. SFPL shall deploy Antivirus, Anti-malware solution to cover all computing devices, including mobile devices/mobile phones. Devices which shall be out of this framework needs to be identified and recorded in ITSC meeting with reasons, probable risks and compensating controls.
- vi. All new applications, modules shall be subjected to IS Audit and User Acceptance Test (UAT) and cleared by CIO before launch. In case of business requirement and meeting minimum level of safeguards, CIO is empowered to permit launch for a limited period (not more than 6 months) and limited user base preferably internal (not more than 100) after completion of User Acceptance Test.
- vii. Baseline Cyber Security and Resilience Requirement shall be implemented in a phased manner. Implementation status to be reported in quarterly ITSC meetings.

## 7. Continuous Surveillance

- i. Vulnerability Assessment (VA), Security Device Configuration, Penetration Testing (PT), Application Security Testing (APPSEC) & Process review shall be performed at least on annual basis for all information system processes and associated production setup. The Asset Owners shall evaluate such vulnerabilities and appropriate measures shall be taken to address the associated risk.
- ii. To anticipate the unknown Cyber-attacks and evolving threat landscape, the SFPL has set up a NOC (Network Operations Centre). NOC shall ensure continuous surveillance through event logs, alerts and advisories received through external relationships. NOC operations shall be headed by officer not below the rank of Senior Manager. NOC Manager shall keep CIO office updated on the abnormal events detected on real-time basis.
- iii. NOC manager shall develop a standard operating procedure (SOP) duly approved by the Steering Committee, for detection of infrastructure logs with any malicious or suspicious events.

## 8. Inventory Management of IT Assets

- i. CIO office shall maintain all Information System Process (updated on quarterly basis) with OS, DB versions, Asset/Process Ownership, Custodians, Criticality and Audit Frequency.
- ii. Complete inventory of IT assets shall be maintained for each process by Process Asset Owners, with hardware Software, version numbers, current state of deployment (e.g. what software is installed on what systems) and the person(s) responsible for the asset to be maintained.

## 9. Maintenance of Information Assets

- i. Asset owners shall issue suitable guidelines through internal communications for acceptable usage of Information Assets.
- ii. IT Head shall ensure enterprise architecture is defined, developed and periodically reviewed so that manual and administrative controls can be converted into automated one especially end-point control, license compliance, patch management, access control, contract management and performance management. Absence of automation should not result in absence of controls even through administrative orders and manual efforts.

- iii. Every Information Asset user shall be made aware of potential hazard of non-compliance of guidelines through continuous awareness programme using Intranet, SMS, Emails, Trainings or any other media. User shall be made aware that non-compliance shall result in suitable disciplinary proceedings on detection by SFPL's HR department.

### 10. Removable Media handling

- i. Removable Media is not permitted to be connected on SFPL's networked computers. In case of business requirement, specific written permission to be obtained from CIO.
- ii. IT department shall implement system related controls wherein USB ports shall be disabled and if enabled after change request process, controls through Data Leakage Prevention tools, Antivirus solution shall be implemented.

### 11. Network Level Security

- i. SFPL network at all levels (LAN, WAN) shall be designed in such a way that no foreign computing resources shall be automatically connected.
- ii. All temporary connections to external agencies within the SFPL or from outside using VPN shall be through Change Management Process. List of all such temporary outside connections shall be maintained by NOC team and requirement shall be reviewed by CIO at least once in a month.
- iii. Host to Host connectivity shall only be based on a specific requirement

### 12. Database Level Security

IT Head shall designate Database Security Manager, who shall ensure Database access is documented for each critical application and process through review mechanism at least once in a month. Asset Owner should validate access level during such review.

### 13. Preventing execution of unauthorised software

- i. Users shall not have authorization to install or uninstall any software (licensed, unlicensed, evaluation version, shareware & freeware) on operational system.
- ii. IT support team is responsible for installation or un-installation of all software from operational system.

## 14. Physical Security and Environmental Controls

- i. Data Centre is to be audited annually to ensure compliance of environmental parameters viz. Power, Air Conditioning, Fire proofing and cleanliness.
- ii. Asset Users/Custodians and Owners shall ensure minimum level of environment parameters as required by OEMs of respective assets are implemented and maintained. Performance shall be assessed periodically through preventive maintenance.
- iii. Physical Access to SFPL's Data Centre (DC), Disaster Recovery (DR) Site or any other central server hosted location even in case of outsourced locations shall be based on requirement and authorization process by Asset Owners. Record of such access shall be maintained for a period of at least 6 months. These locations shall be categorized as Critical Locations.
- iv. All Critical Locations shall be covered through CCTV, DVSS systems and such footage shall be stored for a minimum period of 1 month.
- v. Security Guards shall be deployed at all Critical Locations.
- vi. SFPL shall implement compensating controls like CCTV, Insurance in lieu of CCTV, at Network and Security Operations Centre.

## 15. Securing Customer data

- i. Customer data shall be made available to employees only on “**need to know and need to do**” basis and shall be controlled through username & password-based access.
- ii. Customer data shall be shared to partner organization for 3rd party products only after authorization from customers.
- iii. Sharing or storing of Customer data at Outsourced location shall be made only after Non-Disclosure Agreement and Service Level Agreement is signed with relevant confidentiality clauses.

## 16. Application Security

- i. All Critical applications shall follow principles of secure development, segregation of duties, Application Security Audit, Source Code Audit (if not a standard product).
- ii. Asset Owner shall create document briefing the features of security controls implemented and placed to CIO as part of go live document.

## 17. Creating Awareness

- i. CIO office shall coordinate to create awareness about Cyber Security amongst employees, Board, Customers, vendors, Auditors and Visitors through HR, IT, ADC, Publicity & Audit wings of the SFPL.
- ii. At least one target campaign per month shall be executed using SMS, Email, Intranet, Posters and Contests.
- iii. Cyber Security Day shall be celebrated once in a year

## 18. Internet Access

Devices with direct Internet access (which bypass the firewall security) are not allowed to connect to SFPL's network as user end points.

## 19. IS Outsourcing

- i. Asset owner shall be accountable for any event occurred at partnered arrangements.
- ii. Outsourcing shall be based on assessment of internal capabilities, cost of acquisition & operations and general industry level best practice.
- iii. Partner needs to assure SFPL about their risk compliance through Audit Reports, industry level security standards.

- iv. SFPL shall have full rights to conduct Audit of outsourced environment through internal or 3rd party resources. This clause shall be necessary part of all outsourcing agreements.
- v. In case, SFPL outsources asset management to technical expert agency/vendor agency within their premises, the agency’s personnel shall also be part of continuous surveillance, NDA and SLA driven controls.

**20. Data Leak Prevention**

- i. Customer data collected through Business process, all spreadsheets, word processing files and database backup/exports shall be considered classified.
- ii. Classified information is not allowed to be taken outside SFPL or vendor locations through any media.

**21. Ethical Hacking, Honey pot**

Ethical Hacking, creating honey pots shall be employed only after ITSC approvals.

**22. Baseline Controls**

**(Note: Services which are not relevant may be removed)**

| Control              | Parameter             | Maintained Through       | Document   |
|----------------------|-----------------------|--------------------------|------------|
| Inventory Management | Applications          | CIO                      | Annexure-1 |
|                      | Assets                | Asset Owners             | Annexure-2 |
| Software Control     | Whitelisting Solution | 3 <sup>rd</sup> Party    |            |
|                      | Centralized Control   | 3 <sup>rd</sup> Party    |            |
|                      | Patch Management      | Manual, Automated        |            |
|                      | Exception Authority   | Head-IT, CIO, ITSC       |            |
| Environment Control  | Physical Security     | Guards, Biometrics, CCTV |            |
|                      | Hosting Environment   | Building Management      |            |

|                      |   | System                                       |                       |
|----------------------|---|--|-----------------------|
| Network Security     | Network Architecture                    | Head-IT Network                              |                       |
|                      | Network Assets                          | Manual, Automated                            |                       |
|                      | Configuration                           | Audit  |                       |
|                      | Wireless Access                         | Change Request, MAC, Physical IP             |                       |
|                      | Authorization                           | Manual, NAC                                  |                       |
|                      | Unauthorized Device                     | Detect, SIEM                                 |                       |
|                      | Unusual Activities                      | SIEM   |                       |
|                      | Boundary Defence                        | Firewall, Proxy, IPS, IDS                    |                       |
|                      | Patch & Configuration                   | Audit  |                       |
| Application Security | All Stages of ASLC                      | Policy                                       |                       |
|                      | Source Code Audit                       | Optional                                     |                       |
|                      | OEM Assurance                           | SLA  |                       |
|                      | Security Requirement                    | Asset Owners                                 | Annexure 3            |
|                      | Development, Test & Production systems  | Separate systems                             |                       |
|                      | Secure Coding                           | OWASP standard                               |                       |
|                      | Containerized Mobile Applications       |  |                       |
|                      | Remote Wipe Solution                    |  |                       |
|                      | New Technology                          | Risk Assessment before induction             |                       |
| Patch Management     | Inventory of Patch Requiring systems    | Asset Owners                                 |                       |
|                      | Measurement & Tracking                  | Manual, Automated                            |                       |
|                      | Audit                                   | VA/PT/APPsec/RCA/Secure Configuration        |                       |
| User Access Control  | Encryption of sensitive data at Rest    | Legal and standard Compliance                | Define sensitive data |
|                      | Encryption of sensitive data in transit | VPN, IPsec, SSL                              |                       |
|                      | No admin rights on endpoints            | Endpoint Admin through End point Security SW |                       |
|                      | Centralized Controls                    | Endpoint Admin through End point Security SW |                       |
|                      | Privilege Monitoring                    | <i>End Point security SW</i>                 |                       |
|                      | Invalid Logon Lockout                   | Three  |                       |

|                                   |                                     |   |          |
|-----------------------------------|-------------------------------------|---|----------|
|                                   | Dormant Password Expiry             | 3 Months (Customers)<br>1 Months (Internal-Through Application) |          |
|                                   | Abnormal Logon Alert                | Time, Place abnormality   |          |
| Customer Authentication           | Secure Authentication system        | Policy  |          |
|                                   | Authentication for each transaction | Minimum 2 Factor  |          |
|                                   | Secure Credentials Storage          | HSM, SSM  |          |
| Secure Mail Messaging             | Own                                 | SMTP Gateway  |          |
|                                   | Partners                            | SMTP Gateway  |          |
| Vendor Risk Management            | Accountability                      | Outsourcing Policy  |          |
|                                   | Legal, Policy Compliance            | Continuous Surveillance   |          |
| Removable Media                   | Policy definition                   | Part of Cyber Security Policy                                   |          |
|                                   | Limit Media & information Types.    | Manual & Active Directory Services                              |          |
|                                   | Auto Scan for Malware               | Antivirus Solution  |          |
|                                   | Authorization                       | Blocked by default  |          |
| Real-time Defence                 | Robust Defence                      | Antivirus Solution for all assets                               |          |
|                                   | White listing                       | Proxy access  |          |
| Anti-Phishing                     | Service Subscription                | Cert-In, External agency  |          |
| Data Leak Prevention              | Identification                      | Policy  |          |
|                                   | Prevent                             | Manual, DLP solution  |          |
| Audit Logs                        | Generation, storage and Analysis    | SIEM & NOC  |          |
| VA/PT                             | Periodic Audit                      | As per SFPL's IS Policy   |          |
|                                   | Reporting                           | ITSC (calendar Item)  |          |
|                                   | Participation in Drill              | CIO/NOC Team  |          |
| Incident Management               | Plan                                | Manual Analysis   | Annexure |
|                                   | Reporting & Lessons                 | RCA to ITSC   |          |
|                                   | Recovery                            | BCP   |          |
| Risk Based Transaction Monitoring | FRM                                 | For all customer-initiated delivery                             |          |
|                                   | Transaction Alerts                  | Through SMS & Email   |          |
| Metrics                           | Performance Measurement             | Balanced Scorecard  | Annexure |
| Forensic                          | Tie-up                              | External Agency   |          |
|                                   | Mock Drill                          | Minimum Once in a year  |          |

|           |        |                  |  |
|-----------|--------|------------------|--|
| Awareness | Policy | Awareness Policy |  |
|-----------|--------|------------------|--|

### 23. CYBER CRISIS MANAGEMENT PLAN

**DETECT:**

Following shall act as triggers in declaring CYBER CRISIS by CIO

- Incident of attack detected by NOC, Employees, Partners, third party agencies
- Discovery of compromise through outside agencies and authorities (Media, Customer, Regulators)
- Alert issued by support group & organization or news items

Severity of incident shall be classified as Major or Minor category. Major Incident shall be categorized so, if there is high probability of financial and/or reputation loss.

**RESPONSE:**

| Timeline          | Action        | Sub-action                                | By          | Additional Point            |
|-------------------|---------------|---|-------------|-----------------------------|
| Within 30 Minutes | Communication | Meeting of ISWC                           | CIO         |                             |
| Within 2 Hours    |               | To ITSC members                           | CIO         | For Major Category          |
| Within 24 hours   |               | To Cert-in                                | CIO         | If attack on SFPL's systems |
| Within 24 Hours   |               | To Customers & Employees                  | Asset Owner | After ITSC approval         |
| Within 2 Hours    | Action        | Response Action points shall be finalized | Asset Owner | After ISWC approval         |

**RECOVERY:**

| Timeline        | Action         | Sub-action     | By                          | Additional Point   |
|-----------------|----------------|----------------|-----------------------------|--|
| Within 2 Hours  | Isolation      | Affected Asset | Asset Owner/Network Manager | If it is estimated system is having some degree of vulnerability |
| Within 4 Hours  | BCP            | Activate       | Asset Owner                 |  |
| Within 24 Hours | Log Collection | Affected Asset | Asset Owner/NOC             |  |

**CONTAINMENT:**

| <b>Timeline</b> | <b>Action</b> | <b>Sub-action</b>  | <b>By</b>             | <b>Additional Point</b>          |
|-----------------|---------------|--------------------|-----------------------|----------------------------------|
| Within 48 Hours | Learning      | RCA                | Asset Owner           |                                  |
| Within 48 Hours | Reporting     | To RBI             | CIO                   |                                  |
| Within 48 Hours | Communication | Media              | CIO                   | If Required by Regulators & ITSC |
| Quarterly       | Review        | Incident & Outcome | IT Steering Committee |                                  |

## 24. Glossary

| Sl. | Abbreviation | Description                     |
|-----|--------------|---------------------------------|
| 1   | CSP          | Cyber Security Policy           |
| 2   | CIO          | Chief Information Officer       |
| 3   | IT           | Information Technology          |
| 4   | IPR          | Intellectual Property Rights    |
| 5   | IDS          | Intrusion Detection System      |
| 6   | IPS          | Intrusion Prevention System     |
| 7   | LAN          | Local Area Network              |
| 8   | DDOS         | Distributed Denial of Service   |
| 9   | DLP          | Data Loss Prevention            |
| 10  | WAN          | Wide Area Network               |
| 11  | VPN          | Virtual Private Network         |
| 12  | SOC          | Security Operations Centre      |
| 13  | NOC          | Network Operations Centre       |
| 14  | VA           | Vulnerability Assessment        |
| 15  | PT           | Penetration Testing             |
| 16  | ADC          | Application Delivery Controller |
| 17  | DNS          | Domain Name System              |
| 18  | ITSC         | IT Steering Committee           |
| 19  | ITWC         | IT Working Committee            |
| 20  | UAT          | User Acceptance Test            |

## 25. Other References

| Sl. No. | Reference Clause | Description / Remarks                            |
|---------|------------------|--|
| 1       | SFPL-POL-001     | Information Security Policy                      |
| 2       | SFPL-POL-002     | IT Policies and Procedures                       |
| 4       | SFPL-POL-004     | Business Continuity and Disaster Recovery Policy |

\*\*\*\*\* END OF DOCUMENT\*\*\*\*\*