SREI Equipment Finance Limited

Cyber Security Policy

DOCUMENT RELEASE NOTICE	
Document Title:	**Cyber Security Policy**
Version No.:	**1.5**

REVISION HISTORY

Revision No.	Release Date	Change Details (include Section No., if applicable)	Amended by	Approved by
1.0	14th Feb, 2018	First Release		BODs
1.1	9th Nov, 2019	Cyber Crisis Management Plan (CCMP) added	Aniruddha Mukhopadhyay – CISO	Information Technology Strategy Committee (ITSC)
1.2	21st Jan, 2020	Reviewed by IDRBT	Aniruddha Mukhopadhyay – CISO	IDRBT
1.3	12th Feb, 2020	Approved by the IT Strategy Committee	Aniruddha Mukhopadhyay – CISO	Information Technology Strategy Committee (ITSC)
1.3.1	21st Sep, 2021	Reviewed by Baker Tilly	-	-
1.3.2	7th Dec, 2021	Amendments done based on inputs received from the IT Strategy Committee	IT Team	-
1.3.3	17th May, 2022	Amendments done as per observations of IT Audit 2021-22 and Regulatory / Compliance Review conducted by EY	IT Team	-
1.3.4	6th Jun, 2022	Recommended for approval by the IT Strategy Committee	-	-
1.3.5	26th Jul, 2022	Recommended for approval by the Risk Management Committee	-	-
1.3.6	4th Aug, 2022	Approved by the Core Strategic Committee	-	Core Strategic Committee (CSC)
1.4	4th Aug, 2022	Approved by the Administrator	-	Administrator
1.4.1	27th Apr, 2023	Amendments done as per observations of Risk Assessment activity conducted by Briskinfosec Technology and Consulting Pvt. Ltd.	IT Team	-
	3rd May, 2023	Recommended for approval by the IT Strategy Committee	-	-

	12th Jun, 2023	Recommended for approval by the Risk Management Committee	-	-
	30th Jun, 2023	Recommended for approval by the Core Strategic Committee	-	-
1.5	30th Jun, 2023	Approved by the Administrator	-	Administrator

TABLE OF CONTENTS

1. Applicability

The document applies to SREI Equipment Finance Limited's (SEFL):

1.1 All regular employees (both probationers and confirmed), consultants / advisors

1.2 All trainees and interns

1.3 All SEFL information technology and information processing activities

1.4 All business data stored in a digital form in the systems of SEFL

2. Purpose

Over the last few years, the manifold increase in dependence on technology and its interfacing with external ecosystems to run critical businesses has led to the manifestation of newer risks and threats pertaining to the area of cyber security. The ever-changing nature and frequency of cyber-attacks coupled with their debilitating impact on information systems makes it imperative to develop a comprehensive Cyber Security (CS) Policy specific to the organization.

This policy would cover:

- Vulnerability Management
- Cyber security preparedness indicators
- Cyber Crisis Management Plan (CCMP)
- Sharing of information
- Awareness
- Mobile financial services – Safeguards
- Training

The policy sets out the organizational context of the Cyber Security Framework at SEFL. The purpose of this policy is to outline the framework to protect the IT assets (Data and Infrastructure) of SEFL from cyber-attacks.

2.1 Objective

The objective of this policy is:

- To lay down a comprehensive set of measures and practices that would ensure protection of the organization's IT assets in the cyberspace against cyber-attacks
- To detect such attacks at the earliest
- To respond to such attacks in a consistent manner to minimize the impact in an unfortunate event of a cyber-attack
- To recover the data / systems in a timely manner and to ensure continuity of business

2.2 Scope

The terms SEFL and / or organization would be used interchangeably. This policy is applicable to all critical digital assets of the organization.

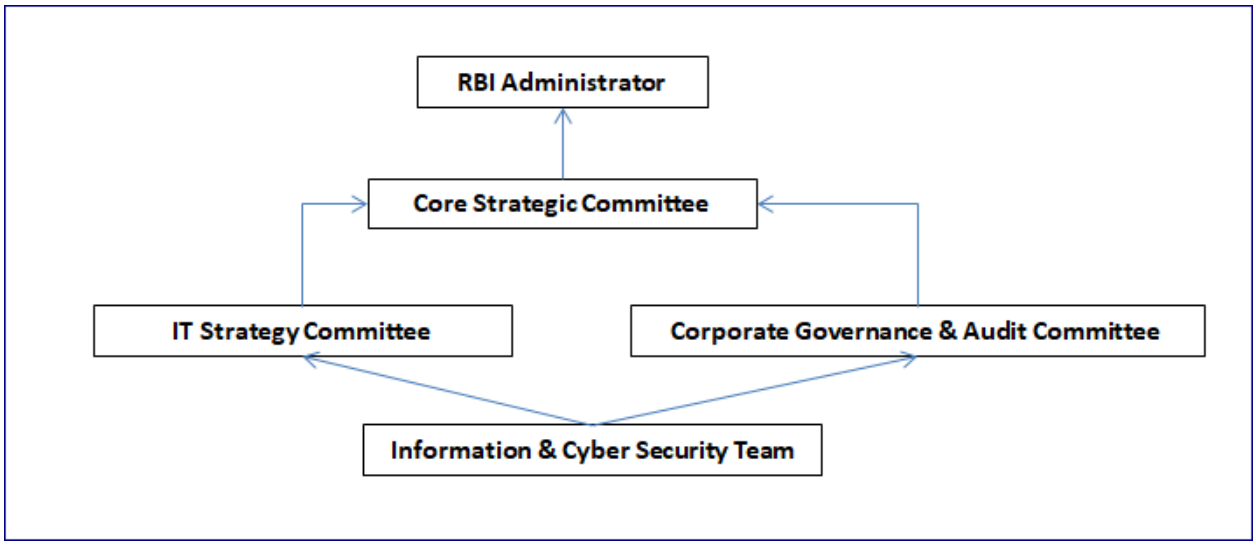
2.3 Periodic review and revision

The Cyber Security Policy shall be reviewed at least once every financial year. The policy may also be reviewed when necessitated by changes in the cyber security risk environment, threat definition or regulatory guidelines.

3. Cyber Security Organization Structure

3.1 SEFL shall have appropriate cyber-security governance consisting of leadership, organizational structures and processes that protect information and information systems, and mitigation of growing cyber-security threats. SEFL's cyber-security governance shall be overseen by its management and senior executives. The Chief Information Security Officer (CISO) shall be responsible for articulating and enforcing the Cyber Security policy. Communication and decision channels shall be deployed to identify and take immediate protective actions during cyber-incidents, to ensure that the cyber resilience of the organization is maintained (Reference: SOC Manual).

3.2 The governance structure for management of cyber security risk shall be helmed by the IT Strategy Committee. The IT Strategy Committee shall have diverse cross-functional members and well-defined terms of reference. At the executive level, the Information & Cyber Security Team shall review the key areas of IT and Cyber Risk and implement relevant control framework. Proceedings of the Information & Cyber Security Team shall be reported to the IT Strategy Committee and the Corporate Governance & Audit Committee.



3.3 The Terms of Reference (TOR) of these committees / teams are as under:

3.3.1 IT Strategy Committee (ITSC)

The composition of the IT Strategy Committee shall be decided as per the Terms of Reference of the Committee duly approved by the Core Strategic Committee (CSC). The IT Strategy Committee should meet at an appropriate frequency but not more than six months should elapse between two meetings.

Roles and responsibilities of the IT Strategy Committee are as under:

a) To provide input to other Committees / Core Strategic Committee and Senior Management regarding IT Strategies and its implementation.

b) To carry out review and amend the IT strategies in line with the Corporate Strategies, Policy reviews, Cyber Security arrangements and any other matter related to IT Governance.

c) To recommend approval of IT strategy and policy documents & ensure that the management has put an effective strategic planning process in place.

d) To ascertain that management has implemented processes and practices that ensure that the IT delivers value to the business.

e) To ensure IT investments represent a balance of risks and benefits and that budgets are acceptable.

f) To monitor the method that management uses to determine the IT resources needed to achieve strategic goals and provide high-level direction for sourcing and use of IT resources – both in-house and outsourced.

g) To ensure proper balance of IT investments for sustaining NBFC's growth and become aware about exposure towards IT risks and controls.

h) Recommending institution of an appropriate governance mechanism for outsourced processes, comprising of risk based policies and procedures, to effectively identify, measure, monitor and control risks associated with outsourcing in an end to end manner.

i) Defining approval authorities for outsourcing depending on nature of risks and materiality of outsourcing.

j) Developing sound and responsive outsourcing risk management policies and procedures commensurate with the nature, scope, and complexity of outsourcing arrangements.

k) Undertaking a periodic review of outsourcing strategies and all existing material outsourcing arrangements.

l) Evaluating the risks and materiality of all prospective outsourcing based on the framework developed by the Board.

m) Periodically reviewing the effectiveness of policies and procedures.

n) Communicating significant risks in outsourcing to the Core Strategic Committee (CSC) on a periodic basis.

o) Ensuring an independent review and audit in accordance with approved policies and procedures.

p) Ensuring that contingency plans have been developed and tested adequately.

3.3.2 Information & Cyber Security Team

Information and Cyber Security Team shall be headed by the CISO and shall consist of the technical team of IT and other stakeholders such as developers or business owners as per the requirement. It shall be operating at an executive level and focusing on priority setting, resource allocation and project tracking and implementation of policies.

Roles and responsibilities of the Information & Cyber Security Team are as under:

a) Lead the development of and updates to a security policy by taking inputs from finance, physical, legal, human resources and business. The organization may outsource the activity of formulation but the ownership shall remain with the CISO.

b) Deployment of Cyber SOC (Security Operations Center) and Security Information and Event Monitoring (SIEM) and continuous monitoring of Information Systems.

c) Protection of Confidentiality, Integrity, Availability and Authenticity of IT systems in the organization by way of deployment of internal and external protection systems like Intrusion Prevention System (IPS), Firewalls, Data Leak Prevention (DLP) solution, End Point Security solution, Web Application Firewall (WAF), Database Activity Monitoring (DAM) solution, Privileged Identity Management (PIM) solution, Email security solution, etc.

d) Developing and facilitating implementation of information and cyber security policies, standards and procedures to ensure that all identified risks are managed within SEFL's risk appetite.

e) Reviewing, maintaining and tracking security incidents and information & cyber security assessments and monitoring activities across the organization.

f) Reporting on information & cyber security activities to the IT Strategy Committee / Corporate Governance & Audit Committee.

g) Proposing best solutions suitable for SEFL for implementation.

h) Reviewing the status of cyber security awareness programme.

i) Conducting periodic security audit / assessment, periodic update of Information Security Policy & Cyber Security Policy and IT Risk Assessment. The Internal Audit department shall be kept informed of all audits which the team envisages to conduct.

j) Ensuring compliance to regulatory and statutory requirements.

k) Review of Information Security and Cyber Security framework in the organization.

l) Identify risks associated with platforms, systems, processes and business impact of key audit observations

m) Review of analysis / RCAs and learnings from major incidents / events in other organizations.

3.3.4 Corporate Governance & Audit Committee

a) Advise the other Committees / Core Strategic Committee on risk strategy and risk appetite, types of risks acceptable considering current and potential future risks and the operating environment.

b) Risk assessment and review to make recommendations to the Core Strategic Committee.

c) Review information / cyber security risks, consider internal controls and review their effectiveness and compliance with laws and regulations.

4. Cyber Risk Assessment and Resilience Framework

SEFL shall adopt a comprehensive and structured cyber-risk assessment and resilience framework. It shall be finalized based on extant frameworks from global standards and best practices. The framework shall be used to calculate the inherent risk of the organization which shall be used to derive the control mechanisms to be implemented. Based on the same, the control parameters shall be reviewed and necessary augmentation shall be done, in case of any identified gaps, by the CISO and shall be recommended to the IT Strategy Committee.

The IT architecture shall be designed in such a manner that it takes care of facilitating the security measures to be in place at all times. The IT architecture shall be reviewed by the IT Strategy Committee and upgraded, if required, as per the risk assessment, in a phased manner based on risk coat / potential cost trade off consideration.

5. Constant Surveillance – Security Operations Centre (SOC)

SEFL shall have a dedicated 24X7 Security Operations Centre (SOC) for monitoring of security events to detect and rapidly respond to cyber-attacks on production (DC) network, application and infrastructure. The SOC shall keep itself regularly updated on the latest nature of emerging cyber threats. In case of any cyber incident, same should be reported to Information & Cyber Security Team. Furthermore, following are the key activities as part of the Security Operations Centre management:

5.1 SOC Building and Cyber Security Capacity Development

5.2 Implementation of:

5.2.1 Real time security log management

5.2.2 Security incident ticket management process

5.2.3 Workflow process analysis

5.2.4 Compliance monitoring

5.2.5 Computer forensics through malware analysis

5.3 Cyber Risk Assessment and threat intelligence management

The SOC team will report to CISO.

6. Network and Database (Infrastructure) Security

SEFL shall implement adequate logical / physical access controls for provisioning and monitoring access to network components and the databases to disallow unauthorized access. Responsibility over such networks and databases shall be clearly elucidated. SEFL shall periodically conduct / participate in simulation drills for various types of cyber-attacks or will be conducted by service provider, as IT infrastructure is outsourced. Conducting unannounced surprise checks can also be useful in assessing the gaps in implementation.

7. Protection of Customer Information

SEFL shall ensure to consistently protect customer information (PII) throughout its life cycle from its origination to destruction, irrespective of whether it is stored / in transit internally within its systems or with customers or with external vendors. Customer data shall be protected in a manner commensurate with its sensitivity through appropriate systems, processes and access by classifying its sensitivity.

SEFL shall conduct application security assessments to ensure that security vulnerabilities, if any, are detected and remediated, so as to protect the organization and its customers from adverse impact. Such assessments shall be conducted by the Information & Cyber Security Team which is the first line of defense and supplemented by similar assessments and ethical hacking exercises conducted by the Information & Cyber Security Team which is the second line of defense. These assessments / exercises may be carried out through qualified and competent professionals / external auditors if deemed necessary. CTO will be ultimately responsible for data privacy / protection in the organization.

8. Mobile Financial Services

SEFL shall develop a mechanism for safeguarding information assets that are used by mobile applications to provide services to customers. The technology used for mobile services should ensure confidentiality, integrity, authenticity and must provide for end-to end encryption.

9. Cyber Security Awareness Initiatives

SEFL shall pro-actively promote cyber-security awareness which would focus on potential impacts of cyber-attacks, covering customers, employees, senior management, employees as well as third party vendors and concerned stakeholders.

10. Cyber Security Preparedness Indicators

SEFL shall identify, with inputs from external agencies if required, cyber-security risk / preparedness indicators to perform continuous assessment of its cyber-security posture.
The following Key Risk Indicators shall be tracked on a quarterly basis:

Sl. No.	Business Process / Domain Description	Key Risk Indicators (KRIs)
1	Backup Management	Backup Completion Success Rate
2		Backup Restoration Success Rate
3	Capacity Management	Average of Network Devices unplanned Downtime Percentage
4		Unplanned Server Downtime
5		Adherence of review of capacity utilization as per the plan
6	Change management	Change Success Rate
7		Unauthorized Change Attempts

Sl. No.	Business Process / Domain Description	Key Risk Indicators (KRIs)
8	IT Business Continuity Management	IT Business Continuity Plan Effectiveness
9	Training and Development	Employee InfoSec Awareness Training Completion Rate
10	Supplier Relationship Management	Number of SLA / NDA breaches that occur in terms of InfoSec for Key IT vendors (Infrastructure, Database, End-user Support & SOC)
11	Patch Management	Patching Compliance for Servers
12		Patching Compliance for Endpoints connecting through MPLS
13		Patching Compliance for Endpoints connecting through any other means except MPLS
14	Access Management	No. of account lockouts
15		Unauthorized access to databases
16		Access Review Planned vs Actual as per Access Review Calendar
17	Asset Management	Mean Time To Recovery (MTTR) of Network Devices
18		Implementation rate of the Asset Disposal Policy of the organization
19	Information Security Incident Management	Number of incidents related to lost or stolen laptops and desktops
20		Rate of successful external intrusion attempts
21		Number of incidents related to privacy breaches or unauthorized access to privacy-related data
22		Number of disciplinary actions taken against employees for violating the IT/IS Policy
23		Phishing email click rate
24	Risk Management	Risk Assessment & Mitigation
25	Vulnerability Management	Compliance percentage of AWS Vulnerability Assessment
26	Internal audit	Closure of Nonconformities in defined time frame
27	License Compliance	License compliance rate for servers
28		License compliance rate for end users w.r.t. OS licenses
29		License compliance rate for end users w.r.t. all other licenses except OS licenses

11. Information and Threat Sharing with RBI

SEFL shall report all types of unusual security incidents (both the successful as well as the attempted incidents which did not fructify) to the Department of Non-Banking Supervision (DNBS), RBI as per the attached template in Annexure II. This is as specified in RBI circular no. RBI/DNBS/2016-17/53 Master Direction DNBS.PPD.No.04/66.15.001/2016-17 dated June 08, 2017 on 'Master Direction – Information Technology Framework for the NBFC Sector'.

12. Cyber Crisis Management Plan (CCMP)

Below is the Cyber Crisis Management Plan (CCMP), covering material crisis scenarios and a mechanism to address all the four aspects pertaining to the same, namely detection, response, recovery and containment.

12.1 Purpose

This document sets out the organizational context of the Cyber Crisis Management Plan (CCMP) in SEFL. It describes what the organization does, how it does it, what factors influence the way it operates and the reasons for the definition of the scope of the CCMP.

12.2 Background

In recent times, cyber-risk has evolved into a key financial and reputational vulnerability and has made quick progress up the risk register. Due to the inherent nature and complexity of a cyber-risk, cyber-crisis should no longer be considered as a glitch. Cyber incidents should not be considered as technical problems and responded to with only technical solutions. In order to combat cyber-incidents, SEFL already has an incident response plan covering the various facets of incident handling. However, in recent times the scope and the prolific nature of the cyber-attacks are far graver and the negative publicity they warrant have gone up substantially. Hence, it has become imperative to devise a comprehensive Cyber Crisis Management Plan (CCMP) that envisages the various facets pertaining to cyber crisis scenarios. CCMP is a framework that outlines how cyber-incidents are managed right from their onset until recovery and is activated once such crisis has been perpetuated. The CCMP provides systematic steps starting from detection of an incident and responding to it leading to restoration of services and containment of the risks arising out of that incident. The objective is to take mitigating measures to proactively detect and prevent cyber-attacks so that the organization is best prepared to respond, restore and minimize the outcome.

12.3 Indicators of Cyber Crisis

12.3.1 Cyber crisis is an abnormal and unsuitable situation that threatens an organisation's strategic objectives, material reputation, impact or viability. It is defined as coordinated, large scale cyber events that result in or have the potential to result in a widespread business or IT outage or disrupt single or multiple infrastructures, services and operations.

12.3.2 The scope of the CCMP shall apply only to material incidents which impact the availability of SEFL's critical applications / services / infrastructure or unlawful publication, obtaining and / or modification of information stored on its IT services. Following are the cyber-incidents (but not limited to) which have the potential to become a crisis provided it satisfies the definition of crisis as aforementioned:

a) Denial of Service (DoS) incidents including Distributed Denial of Service (DDoS)

b) Virus and worm incidents including Malware, Spamware, Ransomware & Cryptoware

c) Hacker initiated incidents which include social engineering attacks (like email phishing, spear phishing, whaling, vishing) and various technical frauds

12.3.3 Systems covered under Cyber Crisis Management Plan (CCMP)

This policy shall cover all the systems (applications, devices and supporting infrastructure) that are accessible using the Internet. Due to the very nature of these systems involving a network that is not directly under the control of the organization, they may cause potential impact if compromised. Hence these systems are considered as "critical impacting systems'' of the organization and covered under the CCMP.

12.3.4 Distinction between Event, Incident and Crisis

a) An 'event' is an observed change to the normal behaviour of a system, environment, process, workflow or person. Examples: Router ACLs were updated or firewall policy was pushed resulting in disruptions of service, etc.

b) An 'incident' is a malicious event that leads to (or may lead to) a significant disruption of business. Examples: Attacker posts company credentials online, attacker steals customer credit card database, worm spreading through network. Incidents are more predictable and can be dealt with through standard pre-prepared and well-rehearsed responses.

c) A 'crisis' may be as a result of an 'incident' – but not necessarily. A crisis is an abnormal and unstable situation that threatens an organization's strategic objectives, reputation or viability; it could be a result of rumours, product defects, adverse publicity, negative social media activities, or actions of employees, distributors or suppliers which reflect poorly upon the organization.

Not every Incident will result in a Crisis (an operational disruption may be transparent to anyone outside the organization). Not every Crisis will be an Incident (adverse publicity, for example, should not disrupt day-to-day operations).

12.4 Cyber Crisis Management Team (CCMT)

The Information and Cyber Security Team shall act as the Cyber Crisis Management Team (CCMT). This team would only be activated when a cyber-crisis scenario occurs and shall act as a decision-making body to take strategic as well as tactical decisions pertaining to handling of crisis scenarios. In the event of occurrence of a cyber-crisis as defined in the earlier section, the Information & Cyber Security Team of the organization shall convene a special Information & Cyber Security Team meeting to initiate the crisis management procedures. It shall meet on a daily basis or at a frequency as deemed fit by it, till the crisis is resolved.

12.4.1 Agenda

The agenda for the meeting will include the following:

a) Assessment of the situation

i. Detection of crisis – causes of the crisis and available analysis thereof

ii. Extent of crisis – applications / infrastructure / systems impacted

iii. Impact of the crisis – business impact, operational impact, customer impact

iv. Direct and indirect impacts

v. Near term and long-term impacts

b) Responses undertaken, effect of response, success or limitations of response and any new proposal (controls) for mitigating, containing and minimising the crisis

c) Communications to be made and via which method:

i. External

- Notification to regulator(s)
- Notification to suppliers and partners
- Notification to insurance firms, if cyber insurance or business disruption insurance applies
- Communication to the media
- Customer communication to corporate and retail clients / institutions
- Government and local authorities e.g. Indian Computer Emergency Response Team (CERT-In) by CISO
- Law Enforcement Agencies by CISO in consultation with Legal Team

ii. Internal

- Employee communication
- Branches
- Customer support (Customer Services Group, etc.)
- Group companies, subsidiaries

iii. Decision such as whether branches need to be kept open on Sundays / holidays to provide an alternative customer support (since internet / mobile / Facebook channels might be unavailable).

12.4.2 Information and Cyber Security Team approved action points with deadlines shall be noted and circulated among teams concerned. The Chief Technology Officer (CTO) or the Corporate Governance & Audit Committee will update the Core Strategic Committee and seek their involvement as necessary.

12.4.3 In case of a scenario where there is possibility of a material reputation impact on SEFL, concerned BCM and Legal teams / members shall be invited for the Information & Cyber Security Team meeting.

12.5 Cyber Crisis Management Process

Cyber crisis management process provides guidelines that can be implemented for the management of cyber security incidents so that restoration of services, infrastructure and / or applications is done as quickly as possible, thereby reducing the adverse impact on business operations. The primary objective

of the procedures is to ensure the highest levels of service quality and availability. The below process workflow defines the activities performed in the event of a cyber-crisis. These phases should not be viewed as distinct and separate stages; instead they might overlap and incorporate each other.

12.5.1 Cyber Crisis Prevention

SEFL shall implement technical and procedural controls for proactive prevention of cyber crisis scenarios. Periodic awareness campaigns shall be conducted to sensitize employees about various cyber security threat vectors and appraising them about cyber crisis management processes and cyber risk vulnerabilities, along with their potential consequences. Specialised advisories and action roadmap shall be shared with technology and business teams.

12.5.2 Cyber Crisis Detection

This phase involves identification of any cyber crisis event and disseminating information pertaining to it to concerned stakeholders. Each of these events shall be detected against a set of Indicators of Compromise (IOC) which shall be defined for every attack category. Both internal (systems for IT related abnormalities, surveillance and information gathering platforms, etc.) and external (open source intelligence, reports from private companies, Government organisations, media houses, etc.) alerts / warnings shall be used to notify the concerned stakeholders of the crisis and then to provide guidance for protecting the systems or recovering any affected systems. Depending upon the nature of incidents and the extent of impact, stakeholders shall be communicated. Depending upon the nature of the crisis, a third party forensic agency may be called upon to perform a detailed root cause analysis of the incident. The purpose of the team shall be to investigate and augment the understanding of the internal team about the full impact of the crisis and its residual risk. The key responsibility of the team shall be to secure the environment, then capture and preserve the evidences in a forensically acceptable manner to be used later for litigation and regulatory submission purposes.

12.5.3 Incident Response

After the detection of the crisis is confirmed – either through internally directed efforts or via notification from a partner / supplier who has been hacked and the impact flows through to SEFL, appropriate team shall engage itself in handling the event. Incidents shall take first priority over other assignments and projects. It would involve in-depth analysis of the incident, followed by both on premise and off-premise incident support, as deemed appropriate and subsequently performing the necessary coordination activities.

12.5.4 Recovery and Restoration

This phase shall involve taking appropriate actions for permanent removal of the vulnerabilities from the system. The basic objective of this phase shall be to repair the control deficiencies so that quick return to normal business operations could be achieved. Depending on the impacted applications / infrastructure, respective business / technology owners shall initiate necessary measures required to restore systems / applications / infrastructure and business operations back to normalcy.

12.5.5 Containment and remediation

Since certain crisis vectors have the ability to propagate to peripheral systems rapidly, they are needed to be stopped from spreading and causing further damage. The objective is to restrict the damages to the ecosystem and minimise the losses arising out of it. Isolating the infected part of the system is often a judicious decision followed by immediate quarantining. A key actionable of this phase shall be to perform a follow-up post mortem of the incident. Concerned stakeholders shall liaison with each other and discuss actions taken and the lessons learnt. A post-facto assessment shall be conducted to ascertain whether control enhancements are required to any system.

12.6 Cyber Crisis Communication Process

There are various internal and external parties that directly and indirectly affect operations of SEFL. During times of crisis, designated groups and personnel of the organization shall handle the communication with internal and external counterparties. A written communication shall be shared on identified causes of the situation, clarifications on the same and the organization's response to the situation, by the Communications Group, in consultation with the Information & Cyber Security Team and other relevant stakeholders from business / technology.

The communication shall be circulated to:

Internal Parties	**Group / Authority that will handle the Communication**
Subsidiaries, Group Companies and Branches (in the international context) / Business Groups	Corporate Communications
Employees	Corporate Communications
IT Strategy Committee / Compliance, Governance & Audit Committee	CTO
External Parties	**Group / Authority that will handle the Communication**
Central Bank, Regulators	Head – Compliance
Corporate, Retail and Institutional clients	Heads of respective business groups
Media, Internet and other communication platforms	Head – Corporate Communications
Central and State Governments, Local Authorities, Financial Institutions and Agencies	Head – Legal, Head – Compliance
Law and Administrative Agencies, Nodal Governmental agencies as required to be notified	Head – Legal, Head – Compliance

Information & Cyber Security Team shall work closely with nodal agencies, such as CERT-In, to assist in mitigating the crisis.

12.7 Testing of CCMP

The CCMP shall be tested periodically for its adequacy. It may be combined with the overall testing of Business Continuity Plan or IT Disaster Recovery Plan or may be suitably tested with the help of table top testing technique. Specific scenarios may be considered for this table top exercise that have been identified or which are based on vulnerability scans, penetration tests conducted earlier or a combination of other factors and strategies.

SEFL may evaluate the possibility of simulating the scenario-based testing to engage everyone in response team in the real-time decision-making process that goes with reacting to a critical cyber incident.

The results of such tests shall be documented along with the lessons learned for future reference. It shall be reported to the IT Strategy Committee.

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

Annexure I – Glossary

Cyberspace	The complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form.
Cyber Security	It comprises of technologies, processes and practices designed to protect the networks, computers, programs and data from any attack, damage or unauthorized access from individuals / organizations.

Annexure II – Template for reporting Cyber Security Incidents


CSIR Form.pdf

Annex - I

Template for reporting Cyber Incidents

1. Security Incident Reporting (SIR) to RBI (within 24 hours):

2. Subsequent update(s) RBI (updates to be provided if the earlier reporting was incomplete i.e. investigation underway or new information pertaining to the incident has been discovered or as per request of RBI):

Basic Information	
1. Particulars of Reporting:	
• Name of the NBFC	
• Date and Time of Reporting to RBI, CERT-IN, other agencies (please mention separately time of reporting to each)	
• Name of Person Reporting	
• Designation/Department	
• Contact details (e.g. official email-id, telephone no, mobile no)	
2. Details of Incident:	
• Date and time of incident detection	
• Type of incidents and systems affected (i) Outage of Critical IT system(s) (e.g. CBS, Treasury Systems, Trade finance systems, Internet banking systems, ATMs, payment systems such as SWIFT, RTGS, NEFT,NACH, IMPS, etc.) (ii) Cyber Security Incident e.g. DDOS, Ransom ware/crypto ware, data breach, data destruction, web defacement, etc.)? [Please complete Annex] (iii) Theft or Loss of Information (e.g. sensitive customer or business information stolen or missing	

1

or destroyed or corrupted)? (iv) Outage of Infrastructure (e.g. which premises-DC/Central Processing Units, branch, etc. power/utilities supply, telecommunications supply,)? (v) Financial (e.g. liquidity, bank run)? (vi) Unavailability of Staff (e.g. number and percentage on loss of staff/absence of staff from work (vii) Others (e.g. outsourced service providers, business partners, breach of IT Act/any other law and RBI/SEBI regulations. Etc.)?	
• What actions or responses have been taken by the NBFC at the time of first reporting/till the time of subsequent reporting?	
3. Impact Assessment (examples are given but not exhaustive):	
• Business impact including availability of services - Internet banking, Cash Management, Trade Finance, Branches, ATMs, Clearing and Settlement activities, etc.	
• Impact on stakeholders- affected retail/corporate customers, affected participants including operator(s), settlement institution(s), business partners, and service providers, etc.	
• Financial and market impact – Trading activities, transaction volumes and values, monetary losses, liquidity impact, withdrawal of funds etc.	
• Regulatory and Legal impact	
4. **Chronological order of events:**	
• Date of incident, start time and duration.	
• Escalations done including approvals sought on interim measures to mitigate the event, and reasons for taking such measures	
• Stakeholders informed or involved	

• Channels of communications used (e.g. email, internet, sms, press release, website notice, etc.)	
• Rationale on the decision/activation of BCP and/or DR	
5. Root Cause Analysis(RCA):	
• Factors that caused the problem/ Reasons for occurrence, Cause and effects of incident	
• Interim measures to mitigate/resolve the issue, and reasons for taking such measures, and	
• Steps identified or to be taken to address the problem in the longer term. List the remedial measures/corrections affected(one time measure) and/or corrective actions taken to prevent future occurrences of similar types of incident	
6. Date/target date of resolution_____ (DD/MM/YYYY).	

Note: All fields are REQUIRED to be filled unless otherwise stated.

Annex to Master Direction- Information Technology Framework for the NBFC Sector

CYBER SECURITY INCIDENT REPORTING(CSIR) FORM		
General Information	Report No:	
1. Contact Information: (Please provide if different from what is reported in Basic Information above) Name of NBFC: Name of the person reporting and Designation: Department Official Email : Telephone/Mobile : 2. Is this a ☐New incident ☐Update to reported incident? • For the first update, please indicate "1. If this is an update to a reported incident, please provide the update number for this update. (X.1, X.2, X.3,X.4, etc. where X is the Report No. Update No: Click here to enter text. 3. What severity is this incident being classified as?		
Severity 1 ☐ Affected critical system(s)/ customer facing applications/systems, crippled Internal network or a combination of the above	Severity 2 ☐ Incident occurred on system or network that could put the NBFC's network / critical system(s) or a combination of them at risk	

4

Annex to Master Direction- Information Technology Framework for the NBFC Sector

Information about the Incident
4. Please indicate the date and time the incident was reported to the RBI. If it is also reported to Other Agencies (CERT-IN/NCIIP), Law enforcement agencies, separately indicate the date and time of such reporting. (Please specify in Indian Local Time (+5.30 GMT)) Reported to RBI - Date: Click here to enter a date. Reported to CERT-IN Date: Click here to enter a date. Reported to NCIIP Date: Click here to enter a date. Reported to ----mention the name of agency Date: Click here to enter a date. 5. Types of Threat/Incident ((Please select more than one, as applicable) ☐ Denial of Service (DoS) ☐ Distributed Denial of Service (DDoS) ☐ Virus/Worm/Trojan/Malware ☐ Intrusion/Hack/Unauthorised access ☐ Website Defacement ☐ Misuse of Systems/Inappropriate usage ☐ APT/0-day attack ☐ Spear phishing/Whaling/Phishing/Wishing/Social engineering attack ☐ Other: Click here to enter text. 6. Is this incident related to another incident previously reported? Choose an item. • If "Yes", provide more information on how both incidents are related. Click here to enter text. • Please provide the reference no. of the previously reported incident. Ref no: Click here to enter text.
Incident Details
7. Please provide details of the incident in the box below. • When was the incident first observed/sighted/detected? Click here to enter a date. • How was the incident first observed/sighted/detected? Click here to enter text. • Who observed?

5

8. Please provide details of the critical system(s) or network(s) that is/are impacted by this incident. Details should minimally include:

-Location, purpose of this system/ network, affected applications (including hardware manufacturer, software developer, make/ model, etc.) running on the systems/networks, etc.

Click here to enter text.

What security software installed on the system currently?

If known, any TCP or UDP ports involved in the incident.

If known, provide the affected system's IP address If known, provide the attacker's IP address

Where relevant, please indicate the Operating System of the affected critical system(s): Choose an item.

- If others, kindly state the OS: Click here to enter text.

9. What is the impact of the attack? (Tick 'one' checkbox for each column)

Customer Service Delivery	(Loss of) Sensitive Information	Public Confidence and Reputation
☐No Impact	☐No loss	☐No Impact
☐Minor Impact	☐Minor Loss	☐Minor Impact
☐Major Impact	☐Major Loss	☐Major Impact
☐Serious Impact	☐Serious Loss	☐Serious Impact
☐Severe Impact	☐Severe Loss	☐Severe impact

10. Does the affected critical system(s)/ network(s) have potential impact to another critical system/critical asset(s) of the NBFC?

Choose an item.

- If "Yes", please provide more details.
  Click here to enter text.

Incident Status

11. What is/are the type(s) of follow up action(s) that has/have been taken at this time?

Click here to enter text.

12. What is the current status or resolution of this incident?

Choose an item.

If it is not resolved, what is the next course of actions?

Click here to enter text.

13. What is the earliest known date of attack or compromise? (Tick 'checkbox' if unknown)

(Please specify in Indian Local Time +5.30 GMT)

Date: Click here to enter a date. Unknown: ☐

14. What is the source/cause of the incident? ('NIL' OR 'NA' if unknown)

Click here to enter text.

15. Has the incident been reported to CERT-IN/NCIIP/ any law enforcement agency/IBCART? Choose an item.

- If "Yes", specify the agency that is being reported to.

  Click here to enter text..

16. Is chain of custody maintained?

17. Has the NBFC filled chain of custody form?

18. What tools were used for collecting the evidence for the incident?

Attack Vectors

E1. Did the NBFC locate/identify IP addresses, domain names, related to the incident

Whether the Indicators of Compromise, list of IP addresses identified from the incident, involvement of the IP addresses in the incident (ex. Victim, Malware Command & Control Servers, etc.), domain names resolved, involvement of the domain names in the incident. (ex. Drive-by-download Servers, Malware Control & Command Servers, defaced website), email addresses identified and their involvement, malicious files/attachments (file name, size, MD5/SHA1 hash, etc.) etc. have been reported in IB-CART/CERT-IN/NCIIP/Law enforcement agencies

****