SREI Equipment Finance Limited

Information Technology Policy

A. DOCUMENT RELEASE NOTICE

Document Title:	**Information Technology Policy**
Version:	**4.7**

B. REVISION HISTORY

Revision No.	Release Date	Change Details (include Section No., if applicable)	Amended by	Approved by
1.0	18th Feb 2013	First Release	-	Sunil Kanoria
1.1	5th Sept 2013	Changed 2.6.1 point 10, 31; Updated Annexure 1	Somak Shome	Sunder Raj Vijaynagar
2.0	18th Aug 2014	Changed sections 1.0 – 9.0 as per ISO/IEC 27001:2013 requirements	Tito Gomes, Somak Shome	Sunder Raj Vijaynagar
2.1	14th Aug 2015	Asset management and security incident management	Somak Shome, Ketan Makhija	Deepak Chatrath
3.0	24th Aug 2016	The two docs "IT-SEC-FW-001_ISMS Policy & Framework_v1.3" and "IT-SEC-PG-001_Information Security Policy" have been merged into a single document "Information Security Framework and Policy"	Pranay Biswas	Information & Cyber Security Steering Committee
4.0	25th October 2017	Board Approval taken	-	Approved by BODs
4.1	28th Jan, 2019	Reviewed. No major changes done or modified	-	BODs
4.2	09th Nov 2019	Separate IT Policy prepared. Added the following Domains: SLA Management & Software Development	Yogesh Kajaria – Head IT	ITSC
4.3	21st Jan 2020	Reviewed by IDRBT	Yogesh Kajaria – Head IT	IDRBT
4.4	12th Feb 2020	Approved by the IT Strategy Committee	Yogesh Kajaria – Head IT	ITSC
4.5	27th Jun 2020	Removal of "Access Control" chapter to avoid discrepancies with the IS Policy	Yogesh Kajaria – Head IT	ITSC
4.5.1	22nd Oct 2021	IT Organization Structure has	IT Team	-

		been modified in line with the current framework. Section on Business Continuity Management modified to include details specific to IT BCP concerning Disaster Recovery.		
4.5.2	7th Dec 2021	Amendments done based on inputs received from the IT Strategy Committee	IT Team	-
4.5.3	17th May 2022	Amendments done as per observations of IT Audit 2021-22 and Regulatory / Compliance Review conducted by EY	IT Team	-
4.5.4	6th Jun 2022	Recommended for approval by the IT Strategy Committee	-	-
4.5.5	26th Jul 2022	Recommended for approval by the Risk Management Committee	-	-
4.5.6	4th Aug 2022	Approved by the Core Strategic Committee	-	Core Strategic Committee (CSC)
4.6	4th Aug 2022	Approved by the Administrator	-	Administrator
4.6.1	27th Apr, 2023	Amendments done as per changes in the IT environment of the organization	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	-	-
4.7	30th Jun, 2023	Approved by the Administrator	-	Administrator

TABLE OF CONTENTS

1. Audience

The document applies to:

1.1 SEFL Equipment Finance Limited (SEFL)

1.2 All regular employees (both probationer and confirmed), consultants / advisors

1.3 All trainees, part time faculties, interns

1.4 All third party contractors (including sub-contractors), suppliers, business partners, vendors and service providers of the above listed SEFL companies

2. Purpose of this Document

This document sets out the organizational context of the Information Technology Management System (ITMS) 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 ITMS.

3. Introduction

SEFL has completed its successful journey of 30 years with a great achievement in delivering excellence in BFSI domain. SEFL has made significant growth of market share in retail businesses, control delinquencies in retail and SME segments, navigated through very tight liquidity in strategic investment, repossessed and sold more equipment than ever and despite all this its treasury was as efficient as ever and has maintained and upheld its values and reputation to make it indispensable in the CE industry.

3.1 Services of SEFL

3.1.1 Infrastructure Business

SEFL offers a range of innovative infrastructure financing solutions to help build a better tomorrow. As a holistic institution, SEFL offers the full gamut of services encompassing fund-based, fee-based and strategic investment services.

a) Fund based

i. Equipment Financing

ii. Project Financing

b) Fee based

i. Project Advisory

ii. Project Development

iii. Investment Orgnisationing

iv. Alternative Investment Funds

v. Insurance Broking

c) **Strategic Investment:**

i. Telecom Infrastructure

ii. Transportation

iii. Power

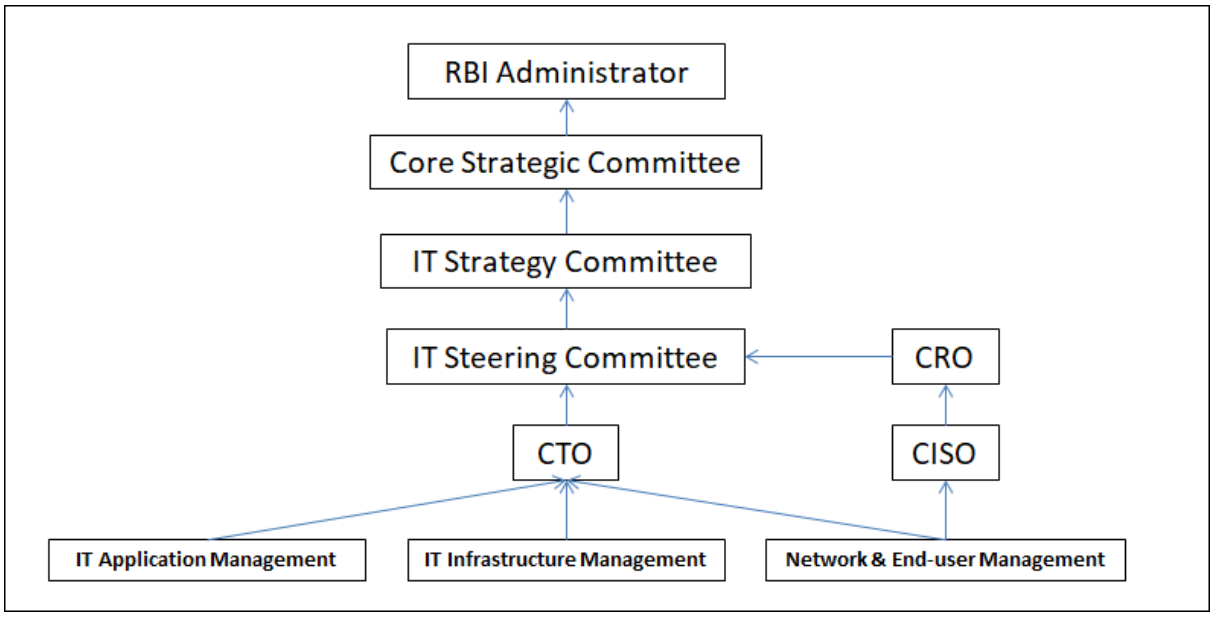
iv. Rentals (Construction, Oil & Gas, Energy)

v. Rural IT infrastructure

vi. SEZ & Industrial Parks

vii. Environment (Water management / Waste management)

4. IT Organization Structure



CTO – Chief Technology officer

CRO – Chief Risk Officer

CISO – Chief Information Security Officer

5. Roles & Responsibilities

Sl. No.	Role	Responsibilities
1	**Information Technology 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. ➢ To provide input to other Committees / Core Strategic Committee and Senior Management regarding IT Strategies and its implementation. ➢ 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. ➢ To recommend approval of IT strategy and policy documents & ensure that the management has put an effective strategic planning process in place. ➢ To ascertain that management has implemented processes and practices that ensure that the IT delivers value to the business. ➢ To ensure IT investments represent a balance of risks and benefits and that budgets are acceptable. ➢ 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. ➢ To ensure proper balance of IT investments for sustaining NBFC's growth and become aware about exposure towards IT risks and controls. ➢ 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. ➢ Defining approval authorities for outsourcing depending on nature of risks and materiality of outsourcing. ➢ Developing sound and responsive outsourcing risk management policies and procedures commensurate with the nature, scope, and complexity of outsourcing arrangements. ➢ Undertaking a periodic review of outsourcing strategies and all existing material outsourcing arrangements. ➢ Evaluating the risks and materiality of all prospective outsourcing based on the framework developed by the Board. ➢ Periodically reviewing the effectiveness of policies and procedures.

		➢ Communicating significant risks in outsourcing to the Core Strategic Committee (CSC) on a periodic basis. ➢ Ensuring an independent review and audit in accordance with approved policies and procedures. ➢ Ensuring that contingency plans have been developed and tested adequately.
2	**IT Steering Committee**	➢ The IT Steering Committee shall operate at an executive level consisting of business owners, the development team and other stakeholders. ➢ Focus on priority setting, resource allocation and project tracking. ➢ Provide oversight and monitoring of the progress of the project, including deliverables to be realized at each phase of the project and milestones to be reached according to the project timetable.
3	**Chief Technology Officer (CTO)**	➢ Responsible for ensuring Confidentiality, Integrity, Availability and Authenticity for Information Technology operations in the organization ➢ Responsible for aligning IT operations with the business objectives of the organization ➢ Responsible for compliance with Data Privacy and Protection as laid down by regulatory bodies / Statute / Government ➢ To ensure compliance as per IT requirements, policy and process from all functions under the scope of IT policy ➢ Ensuring & providing required information to IT team in implementing proactive measures related to information security controls ➢ Ensure end-to-end closure and required follow-up actions resulting from IT incidents with IT operations team ➢ Assisting with investigations / resolution of problems and / or alleged violations of information security ➢ Briefing the forum on current threats and recommended safeguards. Participate in security training programs. ➢ Monitoring of timely implementation of updates ➢ IT Application Management ➢ IT Infrastructure management ➢ Network and endpoint management
4	**Chief Information Security Officer (CISO)**	➢ 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. ➢ Deployment of Cyber SOC (Security Operations Center) and Security Information and Event Monitoring (SIEM) and continuous monitoring of Information Systems. ➢ 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. ➢ 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. ➢ Reviewing, maintaining and tracking security incidents and information & cyber security assessments and monitoring activities across the organization. ➢ Reporting on information & cyber security activities to the IT Strategy Committee / Corporate Governance & Audit Committee. ➢ Proposing best solutions suitable for SEFL for implementation. ➢ Reviewing the status of cyber security awareness programme. ➢ 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 such audits which the CISO / team envisages to conduct. ➢ Ensuring compliance to regulatory and statutory requirements. ➢ Review of Information Security and Cyber Security framework in the organization. ➢ Identify risks associated with platforms, systems, processes and business impact of key audit observations ➢ Review of analysis / RCAs and learnings from major incidents / events in other organizations.

6. Document Confidentiality

This document is confidential and hence would be made available through the organization's Intranet Portals /other similar channels / websites.

7. Objective of the IT Policy

The objective of the IT Policy is to set the guiding principles for establishing IT operational procedures and at the same time to achieve Confidentiality, Privacy, Integrity and Availability of the information and information systems used by those IT Operations. IT Policy should be read in conjunction with the IS (Information Security) Policy.

8. Standards & Procedures

Standards are detailed requirements that need to be met for complying with the IT policies. Separate set of standards have been developed for each policy statement. Standards include measures that need to be taken for mitigating all risks associated with the respective domain covered by the policy statements. Procedures are detailed guidelines of how to implement the measures and who should be responsible for the implementation.

8.1 Objective

8.1.1 To ensure that IT Policy is interpreted correctly and uniformly across the Organization

8.1.2 To provide guidelines for implementation of the policies

8.1.3 To create awareness about policies and assist in policy compliance

9. Scope & Coverage

These policies & standards are applicable to all organization locations including all IT assets, all IT processes, all business processes supported by IT and all employees of the organization.

All services provided by the outsourced service providers including ASP shall also be governed by this policy.

10. Review

IT department will review this policy and standards and procedures every year, based on user inputs, independent review reports, compliance reports or new risk exposure and propose changes wherever required. They will also review and propose changes to the standards and procedures when significant incidents occur in the organization and based on applicable legal and regulatory requirements. All such changes will be approved by ITSC before becoming effective. Review is also to be done at approving authority level.

11. Information / Data Management

11.1 Key Control Objective

Any information related to SEFL and any company-provided information processing system (laptop / desktop / tablet, etc.) is an asset of the company and owned by the company. The company is charged with the protection of information of its clients and its people. In order to secure these assets properly it is vital that the company applies controls that are appropriate to its agreed data classification. Failure to protect this information asset could incur severe financial penalties as a result of legal or regulatory fines, and could potentially damage the company's brand reputation and affect future profitability.

11.2 Controls

The following controls must be put in place within SEFL:

11.2.1 An inventory of all information and technology assets that are classified as important or critical must be created and maintained on an on-going basis.

11.2.2 All information / data should have an identified Information Owner, who is responsible for classifying the importance of the information / data to the business with regard to confidentiality, integrity and availability and the financial impact should it be lost, corrupted, stolen or unavailable. All information must be classified by the Information Owner in accordance with the Data Classification schema, which defines data classification by confidentiality, integrity and availability.

Classification Level	Description
PUBLIC	Information that is available to the general public and intended for distribution outside the Organization. This information may be freely disseminated without potential harm.
INTERNAL	Information that is deemed sensitive due to financial or legal ramifications and which is for use only by authorized Organization employees and auditors, consultants, vendor personnel, legal and regulatory authorities.
CONFIDENTIAL	Information that is proprietary to the Organization and its unauthorized disclosure could adversely impact the Organization, its employees and its customers.
TOP SECRET	Information that is so confidential that leak of such information can severely impact the organization, its employees and all the relevant stakeholders including the customers.

11.2.3 Information owners and the IT department must ensure that data destruction, retention and backups comply with business, legal and regulatory requirements. Service level agreements, procedures and / or software must be put in place to ensure compliance. Data destruction procedures must include logging details of the destruction, including a date and time stamp and the method of destruction.

11.2.4 Information classified in accordance with the Data Classification schema must be labelled appropriately and handling procedures must be developed and implemented for each category of information.

11.2.5 The IT department will be the owner of all physical assets like servers, laptops, desktops, network equipment, storages, etc. An asset inventory to be maintained for these items.

11.2.6 Incidental personal use of Company IT assets is permitted so long as such use does not interfere with Company business, relate to a personal business venture, or otherwise violate this policy or any other policy of the Company and it is brief, limited in volume / number, not disruptive of any Company IT system's function, capacity or throughput or the primary intended uses of such resources, not disruptive of the work environment or productivity, and in compliance with this and all other Company policies including, for example, the Company's solicitation and distribution policy and the Company's policy against harassment and discrimination. The Company reserves both the right and the sole discretion to determine when personal use of Company IT assets exceeds an incidental level, and reserves the right and sole discretion to withdraw permission for personal use of Company IT assets at any time and for any reason.

11.2.7 Sensitive Company information shall not be transmitted via an electronic communication unless secured according to standards established by the IT department, and even then, only to necessary and authorized recipients.

11.2.8 The user name, electronic mail address, organizational affiliation and related information included on all Company electronic communications and all electronic communications that are created, sent, received, transmitted, stored or processed on Company IT assets must reflect the actual originator of the communication.

12. Change Management

12.1 Objective

12.1.1 Enable beneficial changes to be made with minimal disruption to IT services

12.1.2 Establish a standard guideline for identification, categorization and prioritization of changes

12.1.3 Ensure controlled change management by optimizing risk exposure, minimizing the severity and impact, avoid conflict, enabling right authorization & implement standard process & procedure for any change

12.1.4 Ensure real and expected outcome from any change

12.2 Scope

This policy applies to the entire life cycle of service asset & configuration item (e.g. infrastructure, application, utility, document, etc.) which are used for IT service delivery of SEFL and its affiliates, subsidiaries and joint ventures.

12.3 Applicability

This policy is applicable for addition, modification and deletion of any service asset or configuration item that has an impact or will have an impact on established service delivery model.

12.4 Change Management Policy Guideline

12.4.1 All change management requests will involve the following stages:

a) Prioritizing and responding to change proposals from business

b) Cost benefit analysis of the changes proposed

c) Assessing risks associated with the changes proposed

d) Obtaining approval (BRD sign-off) from appropriate authorities for any new development

e) Performing UAT

f) Obtaining necessary approvals before production movement

g) Change implementation, monitoring and reporting

12.4.2 All activities along with responsibility-accountability matrix must be developed, agreed & followed for all change handling. Any exemption to conduct any activity must be properly justified, documented and approved.

12.4.3 Any request for intervention in production must be considered as a request for change (RFC) and executed through change management process. The scope of change management is defined in detail in change management process document.

12.4.4 All RFCs received should be recorded along with a unique identification number. The procedure for logging and recording the change should be documented and followed. (Refer change management process document).

12.4.5 All changes must be reviewed by relevant authority.

12.4.6 For all changes, potential impact of the proposed change must be assessed, reviewed and documented from all relevant service and business aspects. It is recommended to develop and

follow specific impact assessment form to prompt the impact assessors about specific types of change.

12.4.7 Every change should be categorized and prioritized as per change management process guideline.

12.4.8 A formal approval process must exist for every change request under the scope & control of –IT services. A Change Advisory Board (CAB) is the authority to decide on all Change Management requests. CTO will be the convener of CAB.

12.4.9 The operational aspects carrying out Change Management is prescribed in the Standard Operating Procedure (SOP) document, separately prepared and approved by CTO.

13. SLA Management

13.1 Applicability

This policy is applicable for IT Services Outsourcing, including addition, modification or deletion of any service asset or configuration item that has an impact or will have an impact on established service delivery model. Applicability is only to the external vendors who are providing the service.

13.2 Policy

13.2.1 Service Level Agreements (SLA) should be entered into with external vendors for providing services related to management of applications, servers / desktops, networks or data processing. SLA should specify availability and performance requirements (e.g. availability of IT components / applications, response time of applications, restore time for problems, accuracy and integrity of data, expected throughput / output of work, etc.) and establish vendor accountability.

13.2.2 The SLA contract should have enabling clauses for:

a) Monitoring and oversight

b) Access to books and records / audit and inspection

c) Right to conduct audits on the service provider whether by its internal or external auditors or by external specialists appointed to act on its behalf and to obtain copies of any audit or review reports and findings made on the service provider

d) Allowing the Reserve Bank of India (RBI) or persons authorized by it to access the NBFC's documents, records of transactions and other necessary information given to, stored or processed by the service provider within a reasonable time

13.2.3 The CTO should formulate or appoint a person knowledgeable in the concerned area for formulating the Service Level Agreement (SLA) requirements. SLA agreement should cover all the related requirements mentioned in the Outsourcing Policy.

13.2.4 Typical SLA will include the following components:

a) Service objective defining

i. What is the overall objective for establishing the SLA

ii. A description, from the organization's perspective, of functions to be provided by the service provider

iii. Service objective generally is a measure of the quality, speed, availability, capacity, reliability, user-friendliness, timeliness, conformity, efficiency or effectiveness of services

b) Scope of services including:

i. Definition of service provided which must include all the user requirements and / or hardware / software for which the service will be offered

ii. Specifications on number of hours and days that service will be offered, including maintenance and upgrades

iii. References to the current operational methods or quality standards to be considered when defining the service

iv. IT resources needed to provide the service

v. As per Outsourcing Policy, the organization reserves the right to audit the vendors / third-parties and activities performed by them as per the agreement. This can be done by the organization's own team or regulatory authorities like RBI or external third party authorized for the same. SLAs should mention the organization's right to audit in above lines, and should ensure that Security Review / Audit report findings are closed by vendor / third-party as per the SLA

vi. Specification of the number and locations of users

c) **Measurement metrics** – The metrics should be simple and measurable without manual effort and should be used to measure and confirm that the necessary service level objectives have been achieved and act as a predictability of the services. The SLA must encompass the following:

i. Each measurement should logically support a requirement that is linked to objectives.

ii. The SLA should be derived from the Business Impact Analysis which ideally should be reviewed once a year.

iii. Accuracy, Integrity and Service Continuity requirements with tolerance limits for downtimes

iv. If a single vendor is offering more than one service, separation of arrangements must be ensured to deliver the services

v. In case vendor fails to meet the SLA provision of cost recovery by Organization should be in place

vi. Formula for calculating the measurement – SLA should define the method for calculating the acceptable ranges of metrics. It should consider exclusion of the following:

- Exception conditions like failure of hardware / software at customer site not managed by the vendor, service dependencies with third parties, scheduled and emergency maintenance, force majeure.
- Scheduled events that impact service availability (like scheduled maintenance, enhancements)

vii. Frequency and interval of measurement – The measurement period is the time horizon for measuring performance. Typically, the measurement period should be one month. Longer measurement periods give the vendor more opportunity to make up for bad performance. Shorter measurement periods give the vendor a "fresh start" more often. Longer measurement periods mean that more is at stake during any measurement period.

d) **Penalties for non-performance** – Penalties can range from extension of service period, reduction in charges, reduction in charges plus additional compensation and corrective action plan. Penalties should match the severity of the consequences to the Organization if the key performance measures are not met. There must be the right to terminate the contract basis the frequency and severity of the SLA breaches.

e) **Reports** – The SLA should require the service provider to make available clear, useful and timely reports on performance for each measurement period. The SLA should also define precisely what information will appear on the reports, such as exception reports for missed service levels and trend reports for key service levels. The SLA should also require the vendor to conduct a root-cause analysis of service level failures and report the results to the Organization. The reports should be submitted to the Application Owner / Department Head for review.

14. Compliance

14.1 Control Objective

The Company's security policies and standards are rendered ineffective unless they are supported by on-going compliance checks and monitoring. The company may incur financial penalties or suffer damage to its brand reputation if it fails to comply with its legal, regulatory or contractual obligations (RBI Guidelines, SEBI Guidelines, Information Technology Act 2000 and its amendments, Data Security Council of India guidelines, etc.).

14.2 Controls

14.2.1 Responsibility for the identification and monitoring of all regulatory and legislative requirements with respect to IT security within the company is assigned to the Information & Cyber Security Team.

14.2.2 Information owners are responsible for any legal, regulatory or contractual requirements (e.g. data protection, privacy, evidence collection) pertaining to their information or applications and communicating this to IT (custodian of data), Risk Management, Internal Audit and Information & Cyber Security Team.

14.2.3 Appropriate procedures shall be implemented by the IT department to ensure compliance with legislative, regulatory and contractual requirements with regard to the use of material in respect of which there may be intellectual property rights (IPR). Intellectual property rights include software or document copyright, design rights, trademarks, patents and source code licenses. Only authorized, appropriately licensed and commercially available open source software should be installed within the SEFL environment. A record of all software licenses must be kept and updated regularly. SEFL IT department must perform a scan of personal computers and the network at a regular frequency to check for unauthorized and inappropriate software and files, and perform random checks to ensure that such software and files are properly licensed.

14.2.4 All-important records that belong to SEFL should be stored in an appropriate manner to prevent any loss, destruction or falsification, in accordance with legal, regulatory, contractual and business requirements. This can include storing the physical records in fire proof safe, taking data backup, etc.

14.2.5 Users must be deterred from using any of the company's information assets – hardware, software and any infrastructure – for any unauthorized purposes other than what is business. Certain personal use is acceptable to a certain extent which may vary based on the asset, as decided by the Management.

14.2.6 The Information & Cyber Security Team will have the authority to perform compliance checks against the company's security policies and standards, in accordance with agreed procedures. The frequency of such compliance checks will be decided by Information & Cyber Security Team.

14.2.7 A process must be put in place to ensure compliance of IT infrastructure with the company's technical standards. Sample checks must be performed by Information & Cyber Security Team to verify the efficiency of this process.

14.2.8 Audit requirements and activities encompassing checks on production systems must be carefully planned, executed and conducted in accordance with change management procedures to avoid disruptions to the business.

14.2.9 All system vulnerability scanning and audit tools must be securely stored and accessible only by authorized staff. Audit and scan results and data must be protected from unauthorized access and stored in a secure location either electronically or physically.

14.2.10 The IT function should support a robust and comprehensive Management Information System (MIS) in respect of various business functions as per the needs of the business.

14.2.11 All regulatory / supervisory returns should be system driven; there should be seamless integration between MIS system and regulatory / supervisory reporting system.

15. Patch Management

15.1 Policy Statement

This policy is to describe how to establish a routine patch-management procedure and to make it a part of standard operations.

15.2 Purpose and Objectives

Purpose of this policy is to ensure secured patching of SEFL's information systems. Patch management is about mitigating risk to the confidentiality of data and the integrity of systems. Patch management is the most effective tool used to protect against vulnerabilities and the least expensive to maintain.

15.3 Scope of the Policy

This policy is applicable to all the systems (desktops, laptops and servers) which are owned by SEFL, managed by SEFL / others and have standard operating systems running on them.

15.4 Roles and Responsibilities

The IT department is responsible for keeping all systems up to date with the latest patches, including those serviced by outsourced vendors.

15.5 Risk of not adhering to the policy

Risks of not adhering to the policy include security breaches and consequent losses due to the compromise of business sensitive data.

15.6 Policy

15.6.1 Monitoring

a) FMS vendor will monitor security mailing lists, vendor notifications, advisories and websites on a daily basis for the release of new patches.

b) FMS vendor shall use WSUS / SCCM server or other tools given by SEFL to monitor for available patches. Server report can be used to find out the current non compliances.

15.6.2 Impact Analysis and Testing

a) The patch will be tested on test systems prior to application in the live environment. The patches for desktops / laptops will be tested by FMS vendor and that for the servers will be tested by SEFL.

b) Testing of patch will include impact analysis.

c) The necessary test environment shall be provided by SEFL.

d) If impact is major, patch will be approved by the Information & Cyber Security Team after testing and before rollout.

e) Change Management process will be followed till the patch is deployed.

15.6.3 Disaster Recovery / Rollback

The activity of patch application may fail owing to various reasons. This may hamper the availability of the application/device resulting in disruption to business. To ensure that the application / device is available even if patching fails, roll back procedure shall be kept ready before the patch application.

15.6.4 Patching

a) Patches will be applied to the general desktops / laptops by FMS vendor under the supervision of the IT department and to the servers by SEFL.

b) For Microsoft Windows patches, SCCM, WSUS or equivalent application as made available by SEFL shall be used.

c) Servers and desktops must comply with the minimum baseline requirements that have been approved by SEFL Information Technology department. These minimum baseline requirements define the default operating system level, service pack, hotfix and patch level required to ensure the security of the SEFL asset and the data that resides on the system. Any exception to the policy must be documented and forwarded to the Information Security Officer for review.

d) Patches will be applied to the production system preferably during non-business hours.

e) Active patching teams are required to compile and maintain reporting metrics that summarize the outcome of each patching cycle. These reports shall be used to evaluate the current patching levels of all systems and to assess the current level of risk. These reports shall be made available to the Information & Cyber Security Team upon request.

f) OEM support may be needed during or after patching.

15.7 Verification

Following the application of a patch, the respective implementing team will verify the successful installation of the patch and that there have been no adverse effects and maintain records of patch installation. These records may be needed to be shared with the Information & Cyber Security Team upon request.

15.8 Exceptions

Exceptions to the patch management policy require formal documented approval from the CTO. Any servers or workstations that do not comply with policy must have an approved exception on file with the Information Security Officer.

16. SDLC Policy

16.1 Intent

This document provides an overview of the Systems Development Life Cycle (SDLC) process for SEFL. The SDLC process consists of eight phases that help manage a wide variety of activities to conduct projects or automate relevant activities with information technology.

16.2 Introduction

SDLC is not limited to technical activity but actually begins with customer needs and evolves through processes and user requirements to develop a solution or support process. A detailed explanation of SDLC procedures is outlined in a separate document and provides guidance, templates, checklists and examples for successful implementation of this policy. The primary objective of implementing a standardized SDLC policy is to provide coordinated excellent service to support the activities of customers and users within SEFL and to ensure following of best practices within the organization.

16.3 Scope

The first section of the policy explains the purpose, background and basic systems development concepts in order to establish a context for policy description. The end user development methodology, project management practices and management controls make up the SDLC environment to which this policy applies. The SDLC phase concept is further explained to ensure the policy or “ground rules” is understandable by individuals other than technology specialists. A simplified and common framework for implementing SDLC will improve communications and promote coordination across projects throughout SEFL's user community. The eight phases of SDLC are:

16.3.1 Initiation
16.3.2 System Concept Development
16.3.3 Planning
16.3.4 Requirements Analysis
16.3.5 Design
16.3.6 Development
16.3.7 Integration and Test
16.3.8 Implementation

16.4 Roles and Responsibilities

16.4.1 For projects developed internally by the IT Team of the organization, the Program Manager and CTO will be responsible.

16.4.2 For projects developed by vendor and deployed in the company’s IT environment, the vendor is responsible for producing necessary certifications / accreditations, to be further verified by the IT department and CTO.

16.4.3 Program / Project Manager – Program manager and project manager are two terms sometimes used interchangeably but actually differ in their roles. The program manager has overall responsibility for all projects within the program and the project manager is responsible for executing the task elements of the project. Designation of the program manager should be based on whether the project serves a dedicated group or serves an infrastructure role to support a wide user base where no

particular group has ownership of the service or system. In the case of a dedicated type of project or system, the program manager should possess some background from the user perspective to ensure the user processes and requirements are fully represented in the project activity.

16.4.4 Customer – The customer is the ultimate benefactor of the service or information product. The customer needs should provide the primary influence on how the user constructs their operating concept and business processes.

16.4.5 User – The user (individual or group) that conducts the support processes, or uses the automation technology or system, to produce a service or product for the customer. The user has the key role of identifying the business processes and the areas for possible automation (new system) or enhancement (existing system or support process).

17. Adoption of Cloud Services

17.1 Intent

This cloud computing policy is meant to ensure that cloud services are not used without the CTO's knowledge. It is imperative that employees not open cloud services accounts or enter into cloud service contracts for the storage, manipulation or exchange of company-related communications or company-owned data without the CTO's input. This is necessary to protect the integrity and confidentiality of the organization's data and the security of the corporate network. The following guidelines are intended to establish a process whereby employees can use cloud services without jeopardizing company data and computing resources.

17.2 Scope

This policy applies to all employees in all departments of SEFL. 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. If you are not sure whether a service is cloud-based or not, please contact the IT department.

17.3 Policy Guidelines

17.3.1 Use of cloud computing services for work purposes must be formally authorized by the CTO. The CTO will certify that security, privacy and all other IT management requirements will be adequately addressed by the cloud computing vendor.

17.3.2 For any cloud services that require users to agree to terms of service, such agreements must be reviewed and approved by the CTO.

17.3.3 The use of such services must comply with the company existing Acceptable Use Policy / Computer Usage Policy / Internet Usage Policy.

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

17.3.5 The use of such services must comply with all laws and regulations governing the handling of Personally Identifiable Information (PII), corporate financial data or any other data owned or collected by the company.

17.3.6 The CTO decides what data may or may not be stored in the Cloud.

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

18. Data Backup Policy

18.1 Objective

It is the objective of SEFL management to ensure availability of the company's information assets. Hence, SEFL has deployed appropriate backup and restoration procedure to protect important data from being lost in the event of an equipment failure, intentional destruction of data, deletion of data due to human error, or disaster. The purpose of this document is to set in place guidelines to ensure the secure backup and recovery of important data that is stored on the SEFL network.

18.2 Scope

This procedure applies to all data elements owned and operated by SEFL. The data to backup includes all client deliverables, engagement related documents and other internal documents including the financial data of the organization.

18.3 Data Backup & Restoration Policy & Procedures

18.3.1 Risk Assessment

In the absence of proper backup and restoration policy and procedures, SEFL information assets are subjected to the following risks:

a) Risk of loss of information / data because of improper backup or no backup
b) Risk of loss of information due to data restoration failure
c) Risk of loss of classified information due to theft of backup media

18.3.2 Roles and Responsibilities

Role	Responsibility
Application Manager(s)	Define backup scope; approval for new backups / changes to the backup schedule
Backup Administrator	Schedule backup, Monitor Backup and restoration
Backup Operator	Backup activity, monitor backup activity, backup restoration testing
Application User	Application User whose data is being backed up

18.3.3 Server Backup Policy

For the continuity of business operations in the event of failures /disasters, it is essential to have backup copies of the data available. The Information & Cyber Security Team is required to ensure that appropriate backup policies are developed and implemented, for specified IT systems and network devices. The list of specific IT systems and network devices shall be provided by IT Operations teams and agreed with SREI IT management.

a) The following shall be included in the Backup and Restoration Procedure:

i. Extent (incremental, differential, full backup) and frequency (backup schedule) of backups.
ii. Backup of business critical data shall be stored on AWS bucket.

iii. Duration for which data are to be maintained

iv. Maintenance and preservation of backup data

v. Responsibility of backup and restoration for critical data elements / systems.

b) Restoration testing should be conducted for the backed up data at specified intervals to ascertain the integrity and adequacy of the backup.

c) Backup Operator shall store backup logs with appropriate access rights assigned to them. They will carry out a log analysis for all the failed backup and restorations.

d) .All backup data shall have uniquely identifiable labels attached to them and the same needs to be maintained in Backup Activity Log that should be updated on a regular basis.

e) Clearly mention file extensions that need to be backed up.

f) Data residing outside the company premises (e.g., Internet public cloud) should be backed up using a secured communication channel. (All AMI and snapshot backup are in the same account of servers; database manual dump backup goes to RMAN server via transit and sync to S3.)

g) Password of all Backup Administrators / Backup Operators should be as per standard password policy.

18.3.4 Server Backup Procedure

a) Backup Scope

Backup scope shall be updated from time to time by Application Manager.

b) Backup Tool(s) Used

Automated Backup tool: AWS console

c) Backup Device

Storage: AWS console

d) Types of Backup

i) Daily – Daily backups will be performed every day from Monday to Sunday.

ii) Weekly – Weekly backups will be carried out on every Monday for respective week.

iii) Monthly – Monthly backup will be carried out on 1st calendar day of succeeding month.

iv) Yearly – Yearly backup will be carried out after the actual happening of year-end, the calendar date for which will be decided in the Board Meeting.

18.3.5 Daily Backup Policy

Daily backups will be performed every day from Monday to Sunday. Daily backup sets will be retained for 7 days. As per the backup solution it deletes expired save sets automatically

18.3.6 Weekly Backup Policy

Weekly backups will be carried out on every Monday; each weekly backup save sets will be retained for 4 weeks and expired save set as per retention period will be deleted automatically as per backup solution.

On the day of weekly backup, all the daily backup sets will not run.

18.3.7 Monthly Backup Policy

Monthly Backup will be carried out on the 1st calendar day of succeeding month; each monthly backup set will be retained for 365 days and expired save sets will be deleted automatically by backup solution as per monthly backup retention period. On the day of monthly backup, the daily backup and weekly backup sets will not run.

18.3.8 Yearly Backup Policy

Yearly Backup will be carried out after the actual happening of year-end, the calendar date for which will be decided in the Board meeting. Each yearly backup will be retained for 10 years and expired save sets will be deleted automatically by the backup solution as per yearly backup retention period. On the day of the yearly backup, the daily, weekly and monthly backups will not run.

18.3.9 Monitoring

Backups are logged by the Backup Operator on a regular basis; status of backups is recorded in a Backup Activity Log.

In case a backup fails, the logs are analyzed by the Backup Operator, troubleshooting is performed and the backups are restarted. Completeness of backups is ensured through the logs generated. In case of major failure with backups, an incident ticket is logged with the vendor wherever applicable.

Backup Administrator / Backup Operator should have restricted management server console privileges based on their roles.

18.3.10 Documentation

Documentation is maintained by the Backup Administrator / Backup Operator to record the details of the backups to be performed on a daily, weekly and monthly basis, details of the backup schedule, last backup performed, backup start time, end time, etc.

Details of backups are recorded in the Backup Activity Log maintained by the Backup Operator from backup tool report. Status of the backups should be updated based on success / failure of backups. The logs are reviewed on a weekly basis by the IT Operations Head.

A monthly report of the logs should be circulated to the CTO and CISO. The report should highlight backups completed successfully, backups failed, new backups added and media tapes failed, if any.

18.3.11 Archiving

Archived data should be stored in the archive volume and once written, the original files should be deleted to conserve storage space. The archive save sets must not have any expiration date and backup level should always be set to full. Archived data should not be subject to recycling. Data archiving activity should be restricted to Backup Administrator / Backup Operator. Retrieval of archived data should be restricted to read-only permission.

18.4 Server Data Backup Restoration Testing

Restoration testing of backup logs is performed on a need basis on a random selection of bucket. The following points to be kept in mind:

i. The logs to be tested will be selected from the random backup save sets. This will help to understand the backup quality, errors, and validate the data wherever applicable.

ii. As the backed up data has been hashed, rerun the checksum and verify it.

iii. Every write to the backup media, should be read back and verified for integrity wherever applicable.

iv. Periodically perform a complete restoration which has got restoration of entire directories, servers, or applications wherever applicable.

v. Do a test restore to a different computer or server.

vi. Make sure to keep a copy of the install disks for your backup software with your backups. Details of the restoration tests performed are recorded in the Restoration Log.

18.5 Request Based New Backup for Servers

Backups might be performed on specific request from users. Requests for backups should be submitted by business owner/user to the Application Manager through a form, approved on email by respective HoD, Application Manager and IT Operations Head; backups will be scheduled based on the available backup windows. Service request / ticket would be raised accordingly.

18.6 Addition / Modification of Backup for Servers

In order to add new scheduled backup or modify an existing backup, the Application Manager initiates a Change Request - details pertaining to the backup viz. server name, backup details & backup path are to be provided in the requisition. The Change Request is approved by the IT Operations Head.

19. Email Usage Policy

19.1 Objective

To define the guidelines concerning effective implementation and maintenance of SEFL's email system.

19.2 Scope

This policy applies to the usage of the email system of SEFL, which can be in-premise or outsourced, and accessing the same using email client in office or outside, or through push mail devices.

19.3 Applicability

The Email Usage Policy applies to all users of SEFL's email system (can be all regular employees – both probationers and confirmed, consultants / advisors, all trainees, part time faculties, interns, all third party contractors including sub-contractors, suppliers, business partners, vendors and service providers) – anyone who has been given an identity on the system through a mailbox. The users are expected to be familiar with and to comply with this policy, and are also required to use their common sense and exercise their good judgment while using email services.

19.4 Policy Guidelines

19.4.1 Official email shall be used for Company business only.

19.4.2 One individual in the group will have one email ID.

19.4.3 All official mails shall be sent through official email ID only. Usage of personal email sites may be monitored to review if it is being used for official communication.

19.4.4 Appropriate disclaimer(s) must be assigned to emails that are sent outside the company in accordance with appropriate legislation within SEFL.

19.4.5 All incoming and outgoing emails must be scanned to check for viruses, spam, malicious codes, file attachments (where legally permissible) and messages that originate from inappropriate sites or email servers.

19.4.6 All outgoing mail should be classified as per SEFL information classification scheme wherever possible.

19.5 Email ID creation

19.5.1 All employees under the payroll of SEFL having an Active Directory will be eligible for a Srei email ID, provided HR intimation for new user creation is received by IT team.

19.5.2 Approval is required from the authorized person in the Application team for email ID creation.

19.5.3 Email ID naming convention is name.surname@srei.com. The user must change the password during first login.

19.5.4 Consultants / advisors, trainees, part time faculties, interns, contractors, vendors, suppliers, business partners, service providers, etc. are also eligible for Srei email ID on case to case basis. In such cases, approval of the relevant business head, CTO and CFO are needed, and the ID will be temporary for duration of the requirement. Email ID naming convention for such cases will be t-name.surname@srei.com.

19.6 Email access

19.6.1 Email can be accessed from desktop or laptop and mobile device. Google Chrome is the standard browser for using Srei's Google Mail and is given as standard offering to all users.

19.6.2 In addition, email can also be accessed through push email devices like Blackberry and smart phones / tablets using Google MDM application & policy. When Srei email is pushed to personal devices, Srei's corporate policy restrictions will apply.

19.7 Mailbox size

19.7.1 All email users will be facilitated with a total Google space up to 30 GB.

19.7.2 For any crucial business requirement, if it is required to increase the limit for any employee, the IT team would do an analysis for the justification of the request.

19.7.3 Once verified by CTO, the space limit will be increased by a block of size 5 GB after obtaining approval from the HOD and CFO; the CTO will be informed basis the justification.

19.8 Email retention and archival

19.8.1 There should be NO deletion of business related emails without prior permission of HOD.

19.8.2 Users may take back up of their business critical data (including emails) on to AWS WorkDocs or Google Drive.

19.8.3 All outgoing emails from the Srei Domain to external public domains shall be monitored.

19.8.4 Users must judiciously use the mail quota allocated to them and keep deleting old unimportant mails which may no longer be required to free up space. Users must periodically archive / backup their important emails. The IT Helpdesk Team may be contacted for assistance in this regard.

19.8.5 Accountability of sending any unwarranted email / data to unauthorized recipient would rest solely with the concerned employee, who would be liable for disciplinary and audit review.

19.9 Common mailbox creation

19.9.1 Common mailboxes are often required where multiple users need one common identity like, SEFL Employee Communique / SEFL, etc.

19.9.2 Requirement for a common mailbox must be validated by respective HOD and approved by CTO. Continuation of such mailboxes shall undergo periodic validation and approval process.

19.10 Individual user's identity management and control

Individuals are responsible to maintain confidentiality of their company email IDs. Users should exercise caution while subscribing to various newsletters, marketing events, various forums where individual user emails are obtained, as it may lead to spam emails from marketing agencies. In such events, users should first unsubscribe from such subscriptions and notify the IT Helpdesk in case such mailers continue to land up in their mailboxes.

19.11 Managing email records with attachments

19.11.1 Users are expected to send only business related files as attachments, like Microsoft Word documents, Excel spreadsheets, Power-point presentations, PDF documents, text files, picture of assets, etc.

19.11.2 Users should reduce the attachments size by using file compression tool (inbuilt in operating system or separately available) as made available by IT.

19.11.3 The size of a single email with attachment(s) must not exceed the restrictions given in next section. A user must be judicious when sending out such email to multiple recipients, as it will consume the bandwidth and stop / delay delivery of other emails – such email can be sent out in batches of few recipients at a time.

19.11.4 Large emails which exceed the attachment limit must be shared using company arranged facility for same.

19.12 Attachment size limit

The following attachment size limitation for outgoing emails will be enforced in SEFL's mail server by the administrator:

Domain	Max size limit
Within and outside SEFL	20 MB

19.13 Email ID deletion

Separated employees' email access must be removed upon leaving SEFL within 1 day of the employee's last working day (LWD). The email IDs along with the corresponding email file will be deleted by logging a ticket by IT Helpdesk and the same will be assigned to the mail administrator for closure. Only if there is a forwarding request from HR, the mail IDs will be retained for the specific period as per the intimation. Further deletion of such email users will be tracked monthly by Helpdesk through follow-up and reconciliation.

19.14 Data Protection

IT department shall ensure that Data Leakage Prevention measures are implemented in the email solution used, to protect the company's data and customers' privacy.

20. User Data at Endpoints – Management Policy

20.1 Purpose

SEFL is committed to managing information security in accordance with RBI's Guidelines, policies and relevant laws and regulations like the Aadhaar Act, IT Act of India, etc.

This policy outlines how the end user information (data) assets will be managed from the security risks to safeguard the confidentiality, integrity and availability of the company's information and communication technology assets and environment.

20.2 Policy

All information assets will be identified and classified and asset inventories will have to be maintained by every department. Each of the department will classify and handle all information assets in accordance with the SEFL Information Security Classification Framework. The information assets will be disposed of in accordance with the company's policy on Retention and Disposal of Data / Information.

20.3 Responsibility

Within a department every employee will be responsible for data classification and usage of the data that is generated or used by the individual employee during performing his or her official responsibilities in the organization.

20.4 Confidential Data Storage

If there is a requirement of storing confidential data that requires access control, owner of the data or individual requiring storing such data will raise a request to IT. A folder with access control as per the access control list provided by the data owner will be implemented in the file server.

20.5 Data Backup

All data stored in the file server will be automatically backed up every day. As every employee has to keep the data in the file server, backup of the individual systems will be discontinued. The common folder used for Inter department file sharing will not be backed up.

20.6 Data Retention Policy

Unless otherwise stated by the data owner all files will be available for 1 year online and data of more than 1 year till 5 years offline except mails. All regulatory data and information will be available for 7 years online.

20.7 Data Owner's Responsibility

20.7.1 The responsibility of identifying the files which need to be stored in the file server will be with the individual file owners.

20.7.2 Owners should decide and put in the file server only those files which need to be stored as per the business requirement.

20.7.3 No email archive files to be stored in the file server.

20.7.4 The emails which are required to be stored should be converted to PDF format for storage. The attachments can be individually stored along with the email PDF files.

20.7.5 Individual system backups should not be stored in the file server.

20.7.6 If there is any loss of data from the computing device of the end users, the personnel would be solely responsible for the same.

20.7.7 CTO shall approve the Standard Operating Procedure (SOP) for file storage / sharing etc. and circulate to all user departments.

21. IT Capacity Management Policy

21.1 Objective

Capacity Management ensures that IT resources are sufficient for the evolving requirements of the business. It maintains a Capacity Plan which describes the IT resources, roadmap and necessary investments. The Capacity Plan is reviewed at least annually as part of the budget process, and also as part of other processes (e.g. Project Management, Service Management). It is based particularly on the demands and requirements which core businesses express throughout the budgetary year.

21.2 Scope

The scope of Capacity Management covers all significant areas which have a direct engagement in production and support of IT services and which has significant financial value.

The current scope of Capacity Management is primarily focused on, but not limited to, the following areas:

21.2.1 IT computing & processing devices (CPU & memory)
21.2.2 IT storage (SAN & backup storage)
21.2.3 IT network
21.2.4 Software licenses

Every resource entity must be linked with supported service and business function. Based on impact, current status & financial implication, these categories may have certain resource exclusion. Hence, a detailed scoping along with exclusion list should be prepared by Capacity Manager and authorized by CTO.

21.3 Policy Guideline

21.3.1 Identifying requirements

The IT department / Project Managers will identify requirements based on business plans, business requirements, SLAs and risk assessment, incident / problem diagnosis report and communicate the same to CTO.

21.3.2 Quarterly Review

Once a quarter CTO will present the capacity utilization report against baseline to IT Strategy Committee members.

21.3.3 Annual review of capacity plan

The Capacity Plan will be reviewed by IT Strategy Committee at least annually in advance of the budget process. A predefined & authorized format / template must be used for producing capacity plan.

21.3.4 Monitoring

A capacity monitoring solution must be deployed, and report must be presented at each meeting of the IT Strategy Committee. For capacity monitoring, all threshold values must be documented & approved by CTO. Capacity monitoring template for every category must be pre-defined and circulated to respective service delivery manager.

The following values are defined for capacity monitoring and review of resource utilisation whenever a system touches 60% capacity utilisation:

a) Till 60% - Normal range

b) 61 to 85% - Warning

c) 86% and above - Error

21.3.5 Capacity plan update

Any change or incident resolution that requires a capacity change in existing service model must be identified & approved by CTO who must update the Capacity Plan post implementation to reflect the current state.

21.3.6 Gap analysis

A gap analysis comparing the capacity plan to the actual situation must be performed on quarterly basis by CTO along with the Business Department. This report will be presented to IT Strategy Committee. In the event of any significant gaps, an action plan must be produced, approved and implemented.

21.3.7 Trend Analysis

Based on the monitoring & gap analysis data, a trend analysis report must be generated for every service by CTO along with Business Department, which will provide prediction of capacity consumption and procurement requirement for next financial year.

22. IT Asset Disposal Policy

22.1 Objective

To define the guidelines for disposal of IT assets like server, desktops / laptops and other IT equipment and safe disposal of data therein.

22.2 Scope

SEFL owned / controlled old IT assets (refer to table below), irrespective of they being in working or non-working condition, will be disposed of in accordance with this policy. Disposal does not necessarily mean throwing away the asset; it can be re-used through various means, or scrapped.

Asset type	Age at beginning of financial year
Server	7 years
Desktop	5 years
Laptop	4 years
Notebook PC	4 years
Networking equipment	5 years
Tablet PC	4 years
Rented Systems	As mentioned in the contract

The scope also covers disposal of Electronic-waste (E-waste). E-waste can be defined as any discarded electrical or electronic devices / products that cannot be used for its intended purpose any more. E-waste comprises of a multitude of components, some containing toxic substances (such as lead, cadmium, beryllium), that can have an adverse impact on human health and the environment if not handled properly.

22.3 Policy Guidelines

Assets that are more than 'x' years old (as per the above table) must be disposed of in a manner that gives the maximum benefit to SEFL and user of the asset is least inconvenienced.

22.4 Procedures

22.4.1 Disposal Planning and Replacement Analysis

a) An asset disposal committee is made comprising of representative(s) from IT, Finance / Accounts and Administration as nominated by the function heads.

b) At the beginning of each financial year, IT will generate the list of assets which are reaching end of life or end of rent / contract period (as on last working day of the previous financial year). The whole list is analyzed and a replacement plan is created for each asset wherever applicable, with a timeline with an approximate budget and justification along with IT Purchase. Replacement plan should consist of the following:

i. Current list and value of assets with configuration

ii. Proposed replacements with technical configuration
iii. Vendor(s) chosen for replacement
iv. Approximate budget
v. Scrap value to be realized from sale of assets to be disposed
vi. Should also contain name of the person / designation / department / company / location to make the list foolproof
vii. Serial no. of the assets to be disposed with make / model no., etc.

c) The list of assets to be disposed, along with the replacement plan, is sent to CTO and CFO for review and approval.

d) Non-working assets containing sensitive data may require a risk assessment to determine whether the item should be physically destroyed rather than sent for repair or discarded.

e) Inputs from here are also provided to the IT budget for the new year.

22.4.2 Valuation of Stock to be Disposed

a) The approved final list of assets (working, non-working and end of rent) to be disposed of, along with the replacement plan, is forwarded to the Finance team who, with the help of IT, determines a Written Down Value (WDV), wherever applicable, for the said items and the same is documented. The final list of assets to be replaced, along with the replacement plan, is forwarded to central Purchase Committee for approval, post whose inputs the replacement plan is modified accordingly. To complete the above mentioned list in all respects such WDV as confirmed by Accounts should be captured in the list for proper record purpose.

b) On receipt of approval of the replacement plan from Purchase Committee, the sourcing activity is initiated by IT Purchase.

22.4.3 New System Sourcing

a) Once dates for receipt of replacement of the asset is confirmed from vendor, IT Operations makes a plan for each employee (for asset like laptop / desktop / notebook / tablet PC) with probable date of new asset allocation to him / her and if the asset contains data, data removal / backup from existing asset to be carried out by IT operations as per employee's availability.

b) IT Purchase hands over newly acquired assets to stock with proper documents like warranty, etc. On receipt of such new assets IT operations will confirm on invoice the receipt.

22.4.4 Data Back up and Cleansing

a) On the planned date, employee is contacted by IT Service Desk and data stored in the asset as identified by him and approved by his / her HOD will be backed up on central file server. That data will be copied to new asset allocated by IT Service Desk on the same day and the data on the server deleted immediately.

b) Data cleansing is achieved by deleting all information in the hard disk of the asset which should be cleaned with minimum 3pass low level format and relevant evidence should be kept and maintained.

c) For rented assets, all assets to be returned to vendor after proper data back up and data cleansing methodologies.

d) The hard disk of IT equipment being scrapped need to be destroyed / disabled as per industry best practices, including degaussing and puncturing procedure.

e) Special care needs to be taken to protect data privacy, in case of contract termination with outsourced vendors and Cloud service providers.

22.4.5 Disk Wiping Tool(s)

The tool shall support the following:

a) Certified by any Government certifying body

b) Works with Windows XP (with Service Pack 3), Windows Server 2003 (with Service Pack 2), Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Linux and Unix and Mac

c) Works with any drive that works with Windows

d) Erases files, folders and their previously deleted counterparts

e) Should have minimum 3 to 7 pass

22.4.6 Scrapping

a) Any 'working' asset that has not still been sold/auctioned (to vendors/employees/outsiders) or donated, and the assets which are old and in 'non-working' condition (as certified by IT and risk assessed) and thus cannot be re-used – now qualify as E-Waste and will be scrapped through third party vendor as per rates decided by the Purchase Committee, and GREEN certification obtained.

b) The following are to be ensured before E-Waste disposal:

- **i.** All the identified scrapped assets would be tagged as "Scrapped".
- **ii.** If asset contains data and is working, data is cleansed by IT Department
- **iii.** Asset details are removed from IT Asset database by IT Department and accounts book / FAR by Accounts
- **iv.** Intimation to Insurance department by IT Department
- **v.** Intimation to IT FMS partner by IT Department
- **vi.** Intimation to IT Procurement by IT Department for disposal advice
- **vii.** Intimation to Administration by IT Department for issuing the gate pass
- **viii.** Asset Disposal Form is updated by IT Department

c) Disposal planning to scrapping will be completed within the first quarter of the financial year, or as and when needed.

d) The appropriate government bodies, e.g., Ministry of Environments & Forests / Central and State pollution control boards in India, etc. have initiated the process of approving and authorizing E-Waste Recyclers. IT Operations Head shall identify authorized Recyclers with assistance of Legal & Admin functions, publish a list of such E-Waste Recyclers and enter into appropriate agreements covering all aspects of the E-Waste disposal. The E-Waste Recycler of SEFL will then execute as per agreed standard operating procedure.

22.4.7 Warranties

Assets are to be sold / donated (to employees, vendors, agencies, individuals) on an "as is" basis with no warranty or guarantee. This should be included in the documentation for the sale.

22.4.8 Roles and Responsibilities

Roles	Responsibilities
Asset Administrator / Manager	a) Identify asset(s) to be disposed b) Prepare replacement plan c) Update Asset Disposal Form as and when required
IT Purchase	a) Help Asset Manager to prepare asset replacement plan b) Help Finance Team to determine the valuation of asset(s) c) Sourcing of new / replacement assets
CTO	a) Approve disposal of asset(s) and replacement
IT Operations / Service Desk	a) Old system decommissioning (includes data back up and cleansing) b) New asset allocation

23. Supplier Management Policy

23.1 Intent

The purpose of this document is to embed information security in all services related to IT Services, general facilities and infrastructure provided by suppliers to SEFL.

23.2 Review Frequency

This document should be reviewed annually and upon significant change to the organisation's supplier landscape.

23.3 Objective

The objectives of the Supplier Management Policy are:

a) To ensure protection of the organization's information assets that is accessible by suppliers

b) To maintain an agreed level of information security and service delivery in line with supplier agreements

23.4 Scope

A supplier is defined as an entity that provides goods or services to an acquiring entity. They may include but are not limited to 'Outsourcers, Information & Communication Technology (ICT) service providers, ICT product providers, Utility service & product providers'.

This policy applies to all suppliers of SEFL and its Affiliates, Subsidiaries and Joint Ventures together referred to as SEFL, who provide various services including IT services to SEFL, such that SEFL's information assets may be at risk.

23.5 Applicability

This policy is designed for third party suppliers / vendors / partners who have direct or indirect access to SEFL's information assets. In SEFL, information is available in both physical and electronic form. Information categories may comprise of confidential non-public business information, information related to organization's support processes / functions / policies or any information that is not meant for public viewing. The effective implementation of this policy is not limited to third parties but also depends on responsiveness of all interfacing functions of SEFL like business, legal, purchase, finance, IT or any other as applicable.

23.6 Supplier Management Policy Guidelines

23.6.1 Rules applicable to suppliers

a) Any request from Suppliers for access to Srei's information system to be approved by CTO. Principle of least privilege to be followed in all such requests.

b) Suppliers must establish reasonable information security practices to comply with the all applicable legal and regulatory requirements currently in effect in the country of operations and as they become effective.

c) Suppliers must develop and exhibit appropriate physical, technical and administrative safeguards for protecting Srei's information assets.

d) Unless otherwise agreed by parties in writing, supplier will not share, transfer, disclose or provide access to Srei's information, information assets or computing systems.

e) Usage of Srei's information and information processing systems should be only limited to the purpose for which the supplier has been authorized for as per contract. Any information, including the ones those have been reconstructed, will at all times be and remain sole property of Srei, unless agreed otherwise in writing by Srei.

f) If a supplier receives a legal or Governmental request for sharing Srei's information, it must keep Srei informed.

g) Supplier will either return or safely dispose Srei's information if no longer needed or upon contract termination or upon Srei's direction which can be given at any time. Any disposal must ensure Srei's information is rendered permanently unreadable or unrecoverable.

h) Supplier will be solely responsible for all acts of its employees / subcontractors.

i) Supplier may do a background verification of its resources deployed at Srei.

j) Supplier appointed personnel must enter Srei's premises with an appropriate ID proof of its own and / or as issued by Srei authorities. Srei information security policies apply equally to its suppliers as to its employees.

k) Suppliers must agree to permit and facilitate audits of all aspects of their information security management system related to Srei information by Srei or Srei appointed authorities, and must address findings related to such audits in order to preserve the security of information with regard to Srei's security requirements.

l) Data from Srei's production environment must not be used for testing purposes by suppliers. Data to be used for testing must be sanitized or otherwise rendered in such a manner that no meaningful data can be reconstructed that might impact the business.

m) Suppliers must report all incidents involving possible compromise of Srei's information to the concerned authority on an immediate basis.

n) Any supplier holding Srei's business critical information (as defined by Srei) must have standard processes in place to ensure that critical information held can be promptly and efficiently recovered following an emergency.

o) Agreement with supplier should contain specific clauses to protect interest of Srei with regard to Data Protection / privacy acts / guidelines by regulators / Government.

p) An effective system of Log Monitoring to be put in place for all Supplier related access to Information System of Srei.

23.6.2 Supplier Selection Criteria

a) While selecting a new supplier, Srei must consider a number of factors including track record, capability, references, credit rating, personnel issues and size relative to the business being placed, as applicable.

b) Security requirement related to physical / logical access to information assets, Intellectual Properties (both onsite / offsite) by the suppliers / representatives and other relevant rules shall be covered under appropriate NDAs / SLAs / other contractual clauses in the contract.

c) A formal contract must exist for all suppliers irrespective of their size of business. The scope and details of contract document may vary with supplier category but at least cover duration of contract, scope of work, confidentiality clause, right to audit clause (applicable for services, not applicable for COTS products), commercials, obligations and termination clause, service levels

if applicable, jurisdiction, etc. In case the vendor / service provider does not agree to the inclusion of right to audit clause in the agreement, then they must provide a compliance certificate to demonstrate that they are following security best practices related to protecting SREI's data. Any new vendor contracts must be reviewed by Srei's Legal team and documented evidences of such review shall be maintained. Existing contracts must also be reviewed by the Legal team at the time of their renewal.

d) A support matrix and escalation matrix must exist, along with contact details for every supplier.

e) A defined process must exist for selection of supplier as defined under IT Procurement Policy. Vendor Evaluation form can be modified as and when required to capture the supplier credentials from information security prospective.

23.6.3 Supplier Service Control

a) A supplier and contract inventory (SCD) may be maintained by Srei and the same updated as and when required.

b) Srei's relevant policies and information security guidelines will be communicated to the supplier's management.

c) The services, reports and records provided by the suppliers must be regularly monitored and reviewed by the concerned department and signed off.

d) All exchange of information (hard and soft copies) with vendors, contractors, suppliers and service providers should be strictly done as per asset handling guidelines.

e) Service, service scope and contract review should be performed on a regular basis, at least annually for all suppliers, and the same documented. The business / customer feedback, major incidents / problems, escalated issues, performance against each target must be considered here.

f) The support and escalation matrix shared by supplier must be updated, as & when required.

g) Changes of vendors, contractors, suppliers and service providers must be done in a controlled manner, taking account of the criticality of their roles, performance & relationship management status.

h) The service(s) catered by supplier will be subject to risk assessment conducted by Srei IT team.

i) A practice for supplier assessment and rating will be in place based on their capability to exhibit their security and compliance level as per Srei expectations.

23.6.4 Supplier Reviews

Supplier reviews serve to assess how the supplier is performing against the agreed Service Level Agreements (SLA). Supplier review evaluation criteria must include the below categories (indicative list):

a) Performance – e.g. efficiency and delivery of contractually agreed services.

b) Incidents – e.g. events that have negatively impacted the business.

c) Billing – e.g. accuracy and timeliness of billing, order processing, etc.

d) Quality – e.g. supplier responsiveness, customer service, supplier knowledge, etc.

Quarterly review meetings shall be held in order to evaluate these areas. For suppliers on a higher billing slab (amount to be decided by internal stakeholders), monthly review meetings can be held.

----------END OF DOCUMENT----------