SREI Equipment Finance Limited

Information Security Policy

DOCUMENT RELEASE NOTICE	
Document Title:	**Information Security Policy**
Version No.:	**4.7**

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 Oct 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 Information Security Framework and Policy document prepared. Domains added.	Aniruddha Mukhopadhyay – CISO	Information Technology Strategy Committee (ITSC)
4.3	21st Jan 2020	Reviewed by IDRBT	Aniruddha Mukhopadhyay – CISO	IDRBT
4.4	12th Feb 2020	Reviewed by the IT Strategy Committee (ITSC)	Aniruddha Mukhopadhyay – CISO	Information Technology Strategy Committee (ITSC)
4.5	27th Jun 2020	Inclusion of sections from Access Control chapter in IT Policy	Aniruddha Mukhopadhyay – CISO	Information Technology Strategy Committee (ITSC)

4.5.1	22nd Oct 2021	IS Organization Structure has been modified in line with the current framework. Section on Risk Management has been modified as per the Risk Assessment exercise carried out and advised by Baker Tilly.	IT Team	-
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 observations of IT / IS Audit for 2022-23 conducted by Kochar Consultants & Risk Assessment activity conducted by Briskinfosec Technology & Consulting	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 Srei 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 SEFL

2. Purpose of this Document

This document sets out the organizational context of Information Security 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 Information Security Framework. The policy document lays down the Information Security framework, objectives, governance and implementation guidelines to protect the Confidentiality, Integrity, Availability and Authenticity of the Organization's systems, assets and data.

3. Areas of the Standard addressed

This document addresses the following requirements:

3.1 Understanding of the organization and its context

3.2 Understanding the needs and expectations of interested parties

3.3 Determining scope of the IS Framework

3.4 Information Security Management System

4. Context of the Organisation

4.1 Context of the Organization is "business environment ", "combination of internal and external factors and conditions that can have an effect on the organization's approach to its products, services and investments and interested parties." Also, in normal language, this concept is also known as business environment, organizational environment or ecosystem of an organization.

4.2 The organization must determine its external and internal issues which should be relevant to its purpose and can affect its ability to achieve the intended outcome of its information security management system. While determining these issues the organization can refer to establishing the external and internal context of the organization.

4.3 The organizational context of Srei is set out in the following sections. Given the fast moving nature of the business and the markets in which it operates, the context will change over time. This document will be reviewed on an **annual** basis and any significant changes will be incorporated. The IS framework will also be updated to cater to the implications of such changes. The CISO will be responsible to make changes to the process document so long as it confirms to the above policy.

5. Introduction

5.1 Srei has completed its successful journey of 30 years with a great achievement in delivering excellence in BFSI domain. Srei has made significant growth of market share in retail businesses, controlled 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 & upheld its values and reputation to make it indispensable in the CE industry.

5.2 Services of Srei:

5.2.1 Infrastructure Business

Srei offers a wide range of innovative infrastructure financing solutions to help build a better tomorrow. As a holistic institution, Srei 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 Organization
- **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)

6. Management Intent

6.1 The Management of Srei recognizes that Information Security is critical to meet the challenges of providing best-in-class service to its customers as well as to have a sound internal control for its information systems. To this end, full commitment shall be demonstrated by providing a supportive framework to promulgate this policy and promote a security culture.

6.2 The Management shall provide evidence of its commitment to the establishment, implementation, operation, monitoring, review, maintenance and improvement of the IS framework by:

6.2.1 Establishing an Information Security policy

6.2.2 Establishing roles and responsibilities for information security

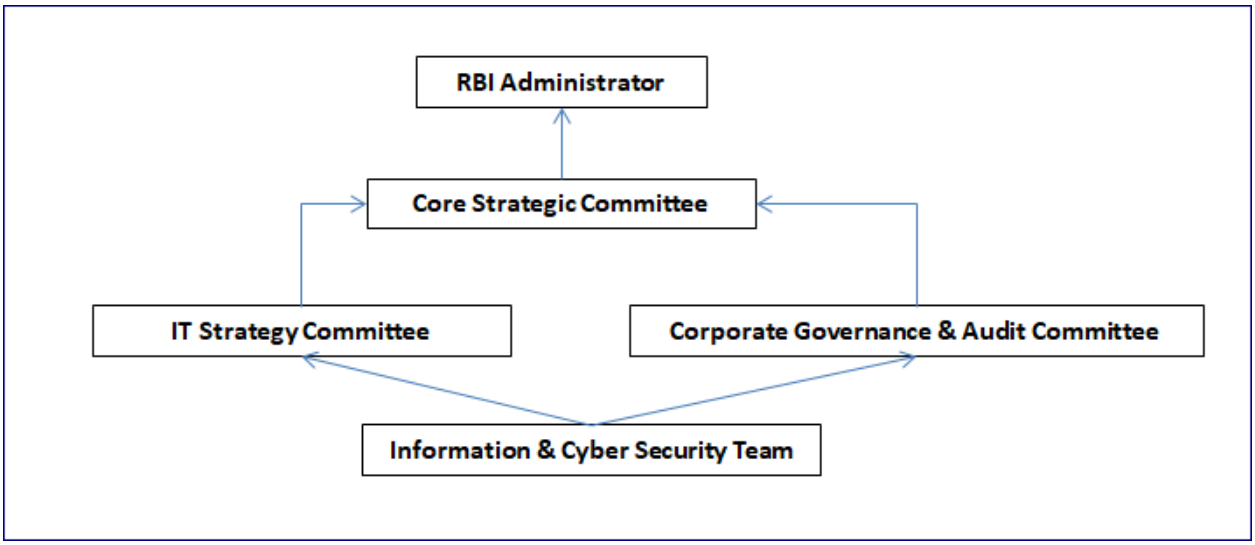
6.2.3 Communicating to the organization the importance of meeting information security objectives and conforming to the information security policy, its responsibilities under the law and the need for continual improvement

6.2.4 Providing sufficient resources to establish, implement, operate, monitor, review, maintain and improve the IS framework

6.2.5 Deciding the criteria for accepting the risk and acceptable levels of risk

7. Organisation Structure

This chart refers to the information flow in the organization regarding the information and cyber security.



8. 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.	**Corporate Governance & Audit Committee (CGAC)**	➢ 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. ➢ Risk assessment and review to make recommendations to the Core Strategic Committee. ➢ Review information / cyber security risks, consider internal controls and review their effectiveness and compliance with laws and regulations.
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 audits which the 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.
5.	**Information System (IS) Audit**	➢ IS Audit shall form an integral part of Internal Audit system of the organization. ➢ IS Audit shall also evaluate the effectiveness of business continuity planning, disaster recovery set up and ensure that BCP is effectively implemented in the organization. ➢ IS Auditors should act independently of the Management. ➢ The organization shall adopt a proper mix of manual techniques and CAATs (Computer Assisted Auditing Techniques) for conducting IS Audit.

9. Needs and expectations of interested parties

An interested party is a person or group that has a stake in the success or performance of an organization. Interested parties may be directly affected by the organization or actively concerned about its performance. Interested parties can come from inside or outside of the organization. Examples of interested parties include customers, suppliers, owners, partners, employees, unions, bankers, or members of the general public. Interested parties are also referred to as stakeholders.

9.1 Legal and regulatory bodies

High ethical standards are in the long term interests of the company as a means to make it credible and trustworthy, not only in day-to-day operations but also with respect to longer term commitments.

9.2 Customers

Srei maintains a high profile clientele consisting of customers from different sectors. While sharing personal & business data with Srei, customers always expect that the integrity, availability & confidentiality of their information will be assured.

9.2.1 Srei has adopted a strong security culture across the organization to meet customer expectations.

9.2.2 Regular audit by internal security teams & external experts are conducted to check the compliance fulfilment.

9.2.3 Security breaches are strongly handled with reactive & proactive measures to enforce & encourage the best suitable security structure for service provision.

9.3 Top Management

Policy statements specify the relationship between remuneration and performance and include measurable standards that emphasize on the long-run interests of the company over and above short-term considerations.

9.4 Suppliers

Srei depends on various suppliers for strategic, business, operational & logistic support. While working through this joint relationship, Srei has always looked for trustworthy, secured, long-term, value-driven relationships with its vendors. The same is expected from vendors too for meeting this objective.

9.4.1 Security requirement related to physical / logical access to assets, Intellectual Property (both on-site /off-site) by the vendors / representatives get covered under appropriate NDAs / SLAs / other contractual clause in the contract.

9.4.2 A third party policy is developed and is followed for Suppliers to comply with organizational / corporate standards, guidelines, and requirement particularly those which are corporate legal, finance, purchase, security ensuring a consistent, seamless relationship between both the parties.

9.4.3 Background verification and risk assessment is carried out prior to vendor selection.

9.5 Partners

Srei has partnered with leading infrastructure sector players to deliver innovative solutions to meet the needs of the customers. Srei's partners represent some of India's and world's leading infrastructure companies.

9.6 Employees

Employees of Srei have an important role to play in ensuring security of information assets of the organization. Security responsibilities should be maintained during and post-employment with Srei.

9.6.1 While joining employees are guided through an NDA which states about employee's responsibilities with regards to security in Srei.

9.6.2 Employees are guided through Code of Ethics as applicable.

9.6.3 Employee Security Handbook has been prepared that clearly specifies security roles & responsibilities of employees in their daily operations. It also gives an insight into the reasons for implementing various security controls. Most importantly, it guides employees in avoiding unintentional violation of a security policy.

9.6.4 Security awareness training & awareness programs are conducted at regular intervals.

9.7 Investors

Investors are particularly interested in the information related to the present and future performance of the enterprise.

10. Information Security Policy Statement

10.1 Objective

The objective of information security is to ensure protection of Confidentiality, Integrity, Availability and Authenticity of IT operations in the organizations, ensure business continuity and minimize business damage by preventing and minimizing the impact of security incidents.

10.2 Policy

10.2.1 The purpose of this Policy is to protect the company's information assets like hardware, software, information, utilities and manpower from all threats, whether internal or external, deliberate or accidental, and to ensure data privacy and protection for all stakeholders.

10.2.2 It will be ensured through this Policy that:

- **a)** Information will be protected against unauthorized access
- **b)** Confidentiality of information will be assured
- **c)** Integrity of information will be maintained
- **d)** High Availability of IT services are made available to all stakeholders
- **e)** Identification and Classification of Information Assets are done
- **f)** Segregation of functions are done
- **g)** Role based Access Control is practiced
- **h)** Personnel Security is ensured
- **i)** Physical Security is ensured
- **j)** Maker-checker practice is available for operations
- **k)** Incident Management procedures are documented and practiced
- **l)** Trails are available and monitored
- **m)** Public Key Infrastructure (PKI) is available
- **n)** Organisation migrates to IPv6 platform as per National Telecom Policy issued by the Government of India in 2012
- **o)** Regulatory and Legislative requirements will be met
- **p)** Business Continuity plan(s) will be produced, maintained and tested
- **q)** Information Security training will be available to all staff
- **r)** All breaches of Information Security, actual or suspected, will be reported to and investigated by Information Security Officer (ISO)

10.2.3 Risk assessment will be done as per organizational Risk Assessment Procedure

10.2.4 Business requirements for the availability of information and information systems will be met.

10.2.5 The role and responsibility for managing information security, referred to as the ISO will be performed by CISO.

10.2.6 The ISO has direct responsibility for maintaining the Policy and providing advice and guidance on its implementation.

10.2.7 All managers are directly responsible for implementing the Policy within their business areas and for adherence by their staff.

10.2.8 It is the responsibility of each employee to adhere to the Policy.

10.2.9 Compliance with the Information Security Policy is mandatory.

10.2.10 The Policy is made relevant, accessible and understandable and is communicated throughout the organization.

11. Information Security Objective(s)

The Information security objectives of Srei are as follows:

11.1 Protection of IT systems from external and internal threats

11.2 Protection of data / privacy of all stakeholders

11.3 Reduction in Information Security Incidents

11.4 Mitigation of Risk

11.5 Information Security awareness

11.6 Information Security Compliance

11.7 Compliance with rectification

12. Scope Statement

The management of Information Security at Srei Equipment Finance Ltd. applies for providing data centre operations and related IT services to group companies (*which include IT security, application management, help desk service, messaging and collaboration service, service monitoring and measurement*) supported by centralized support function of HR and training, physical security, administration and legal.

13. Framework of Internal Controls

The following sections outline the security control objectives and controls to be implemented within Srei.

13.1 Information Security Policy

13.1.1 Key Control Objective

It is the policy of Srei that its information assets be protected from all types of threat, whether internal or external, deliberate or accidental, such that the Srei brand is protected; confidentiality of information is maintained; integrity of information can be relied upon; information is available when required; all statutory, regulatory and contractual obligations are met; and access to information assets is granted only for justified business needs. Individual users of information assets will be identifiable, accountable and may be monitored in their use of those assets.

13.1.2 Controls

a) Srei security organization will use this policy as a basis for compliance audits and security risk analysis.

b) No exception to the controls outlined within this policy is permitted with the exception of those controls identified as not applicable through the application of a formal security risk assessment process, as approved by the Srei Leadership under the advice of the Information & Cyber Security Team. No exception is permitted to the controls required in the case of a security risk analysis finding without the written approval of the relevant Information Owner, and approval of the Srei Leadership is required in the case of an exception to the

controls required to remediate a compliance audit finding. Appropriate documentation will be maintained as long as necessary to support any deviation from controls.

c) The Information & Cyber Security Team will coordinate an annual review of the Information Security Policy and publish agreed amendments in accordance with the defined IT governance process.

d) An on-going process to develop and maintain further or more detailed comprehensive information security policies, standards and guidelines, must be established and implemented and shall include development, review, approval, and publication. These policies, standards and guidelines must be reviewed periodically and in the event of any significant change, to ensure that Srei information technology resources are adequately maintained and protected.

13.2 Organization of Information Security

13.2.1 Key Control Objective

In order to manage and control the implementation of information security effectively within the Srei, it is critical that an information and technology security organization be implemented. Ratified and supported by Srei Leadership, such an organization will play an oversight role of managing the IS framework of the company.

13.2.2 Controls

a) The IT security organization must comprise of a group of security professionals with demonstrable security knowledge, appropriate to the company's security objectives and its size.

b) The IT security organization must have clearly defined roles and responsibilities and these responsibilities will be governed by a RACI (Responsible, Accountable, Consulted and Informed) matrix.

c) Information security must be included in the approval process governing the introduction of any new hardware and software.

d) Responsibility shall be assigned by Srei security organization for the identification of the requirements for confidentiality and non-disclosure agreements, where appropriate and review them regularly.

e) Responsibility shall be assigned by Srei security organization for the maintenance of contact with local groups (e.g. local authorities, industry regulators) that have a significant impact on the security of the local company and its ability to adhere to local legislation.

f) A risk assessment must be performed by the Srei security organization prior to allowing a third party to connect to the Srei network or when creating a remote access solution for third party connectivity (e.g. if implementing multiple third party connections, it is advisable to implement a system that enables secure remote access).

g) Third party logical access to Srei information and systems must be authorized by the information owner of the data or system(s) and be restricted to a pre-determined timeframe and shall be approved by the CISO.

h) Security controls must be put in place restricting the third party access and visibility only to the areas of the Srei network that is required for them to perform the service(s) specified in their contract of engagement with the company. Audit logs showing all access by the third party to the Srei network must be created and stored for periods as required by various regulations / statutes, and reviewed periodically for inappropriate or unauthorized access or access attempts. Where vendors have been granted administrator access for the

purpose of problem resolution, passwords must be changed immediately upon completion of the task, if possible. Access must be either from a secure terminal within the Srei network, direct dial-in modem enabled for the purpose, filtered Internet access (by source/destination IP addresses and ports) enabled during problem resolution or direct serial connection. Internet based non secure connection for the problem resolution is not acceptable. A regular monitoring mechanism should be put in place to ensure compliance to the above.

i) Third parties contracting with Srei who require access to Srei IT resources, must clearly state their explicit agreement to adhere to the Srei information security policies and standards and acknowledge that Srei reserves the right to review their adherence to these policies and standards. The contract must be reviewed by appropriate legal representatives for Srei.

j) An authorized individual from the third party must sign, on their behalf, a non-disclosure agreement (NDA) prior to Srei granting the third party access to the Srei network. Individuals within the third party who will have access to the Srei network must also sign an agreement to abide by the rules of Srei with regard to the use of Srei resources and information prior to accessing the network; the ownership and responsibility for dissemination of such agreements belong to the security organization. Templates for NDAs and resource access policy statements must be reviewed by appropriate legal representatives for Srei.

k) Prior to appointing an external service provider for important or critical services, reasonable due diligence must be performed of the adequacy of their information security controls. This also may include a review of their financial stability and ability to provide the proposed service. In addition, due diligence must be conducted prior to hosting data with a third party.

l) All third party providers of critical services which require high availability must have an associated SLA which covers the following, but not limited to: business continuity, disaster recovery planning, security controls, service definitions, delivery levels. Such agreements must be reviewed periodically for their effectiveness.

m) All third party service providers should be subjected to external Information system Audits at regular intervals and report made available to SREI.

n) Srei should assign responsibility for the monitoring and review of services, reports and records provided by third parties, including but not limited to the outcome of any BCP testing conducted.

o) Changes to the provision of services must be governed using an appropriate change management process and risks should be re-assessed, where appropriate, taking into consideration the criticality of the information systems and processes involved.

p) Security incident management procedures must be developed and agreed between Srei, local legal representation for Srei, and the third party responsible for the management of any security incidents; these must include roles, responsibilities and reporting and escalation procedures.

q) CISO will be responsible for

- **i.** Ensuring compliance of Information Security policy in the organisation
- **ii.** Approving tie up with all third party service providers
- **iii.** Approving Change management requests

iv. Conducting training programs to promote Information Security in the Srei Group

v. Report incidents & review risks & associated threats

vi. Report the same to the ISSC

The CISO will be assisted by the Information & Cyber Security Team to carry out his responsibilities.

14. Human Resource Security

14.1 Key Control Objective

One of the single largest objectives is to protect the company's information and technology assets from human error, lack of knowledge and maliciously failing to implement basic security steps when processing or storing company and client data. Srei must implement the following controls to guard against such threats.

14.2 Controls

14.2.1 The job description of the users shall explicitly state their relevant security responsibilities.

14.2.2 Prospective regular employees must be screened prior to being offered employment within the company. Background verification shall be done to check the completeness and accuracy of information supplied by candidate and shall include, at the least, all educational / academic credentials, past employment records (last three, wherever applicable), completion of last employee exit formalities (release letter / resignation acceptance), etc. Last designation, last drawn salary, dates of employment, reasons for leaving and eligibility for rehiring shall be checked in particular. Confirmation of photo identity to be done through at least two of the following valid identification records: Ministry of Finance (GoI) issued PAN Card, Ministry of External Affairs (GoI) issued Indian Passport, Election Commissioner (GoI) issued Voter ID card, and State Motor Vehicles Department issued Indian Union Driving License. Criminal background should be checked for the personnel with privilege access at the time of onboarding.

14.2.3 HR shall ensure that all vendors contracted to supply services to Srei shall follow similar checks and vetting process while recruiting staff for Srei.

14.2.4 The terms and conditions of employment / contract with Srei shall mandate compliance with Information Security Policy by all users. This shall include a clause requiring the users to protect the confidentiality of information, both during and after the service or contractual relations with Srei.

14.2.5 All users must be made aware of their security responsibilities to the company through one of Acceptable Use Agreement required to be mandatorily signed by them, the Employee Information Security Handbook and the induction training on Information Security awareness within the first 30 days of on boarding.

14.2.6 All staff must receive regular communications about their information security responsibilities and opportunities for further security training.

14.2.7 Srei management shall ensure that all employees, contractors and third parties adhere to security policies, procedures and standards. Procedures must be put in place that address failure to comply with such policies, procedures and standards. Any employee found to have committed a serious security breach shall be subjected to a formal disciplinary process based on Srei personnel security policy.

14.2.8 Responsibilities for performing changes to or termination of employment shall be clearly defined and assigned. Procedures must be implemented to manage cases where staff or contractors change positions or leave the company (including recovery of property owned by the company such as computer equipment, keys, identity cards and access cards).

14.2.9 All assets owned by the company and used by individuals such as employees, contractors and third parties shall be returned upon termination of employment, contract or agreement. All employees must declare their personal computing or IT assets to Security Desk while entering office premises.

14.2.10 Access rights of all employees, contractors and third parties to the company's systems, applications and infrastructure shall be revoked upon termination of employment, contract or agreement, or amended appropriately upon any change of roles. This right also extends to the reduction or removal of access in the event of a security investigation or gardening leave. The Human Resources Management System (HRMS) deployed in the organization should have real-time or near real-time interface with IT systems to ensure automatic revocation of user privileges to achieve the above.

14.3 IT Training & Awareness Methodology

There are two types of training conducted: IT awareness training & Subject matter training

14.3.1 Preparation of IT Awareness Training calendar & Content

a) Conduct assessment among select employees to understand current level of awareness

b) Create content for new joinee induction, Computer-Based Training (CBT) & classroom training; Security handbook to be given to all employees mandatorily

c) Audience for this content include employees (all grades), third parties, contractors

d) Content to include, among others, topics on IT Act of India and PII, Data Privacy and Cyber Security

e) Content to be made in various forms – presentation deck, video, flash file, voice over (subject to discussion and agreement)

f) Content to be based on role, grade, risk (subject to discussion and agreement)

g) Devise plan / calendar when and how to share and distribute these contents with audience over the next one year (12 months)

h) Channels of distribution include email circulars, handouts, desktop artifacts, quiz, workshop, Intranet / web portal, movie show, newsletters, posters, training manuals and presentations

i) All geographic locations (including branches) to be covered

14.3.2 Preparation of IT Subject Matter Training calendar & Content

a) Training can be of two types – Internal & External – depending upon the business requirement

b) Depending upon the business requirement the mode of training i.e., whether internal or external is decided

c) Training calendar is prepared basis the requirement and circulated to all stakeholders over the next one year (12 months)

d) For internal training, the content is prepared by the trainer and is approved by HOD

e) For external training, the content is given by the external training institute

f) Audience for these trainings are selected basis self-nomination approved by their respective HODs

g) All geographic locations (including branches) to be covered

14.3.3 Measuring the effectiveness of the training / awareness program

a) At the end of one year, measure impact / effectiveness (in terms of attendance or participation, awareness and understanding) by conducting mystery test or other form of assessment among same set of employees

b) Conduct feedback survey from selected audience

14.3.4 Providing awareness on information and cyber security to customers and vendors

Awareness on basic Information and Cyber Security related topics to be provided to customer and vendor base of Srei at a regular interval basis by various means like:

a) Mailers

b) Newsletters

c) Highlights in the customer portal

d) Quizzes

e) Online Modules, etc.

15. Access Control Policy

15.1 Objective

The purpose of this document is to define who may access the IT services, facilities and infrastructure provided by SREI, and to describe the logical and physical access conditions to those IT services, facilities and infrastructure items.

15.1.1 The objectives of the Access Control Policy are:

- **a)** To communicate the need for access control.
- **b)** To establish specific requirements for protecting against unauthorized access.
- **c)** To create an IT infrastructure that will facilitate data sharing without compromising security.

15.1.2 The access control should be based on IAAA principle:

- **a)** Identification
- **b)** Authentication
- **c)** Authorization
- **d)** Accountability

15.2 Scope

This control applies to all systems, people and processes that constitute the organisation's information systems, including employees, suppliers and other third parties who have direct access to SREI's systems.

15.3 Business Requirements of Access Controls

15.3.1 The control of access to the organization's information assets is a fundamental part of a defence in depth strategy to information security. In order to effectively protect the confidentiality, integrity and availability of classified data it must be ensured that a comprehensive mix of physical and logical controls is in place.

15.3.2 The policy with regard to access control must ensure that the measures implemented are appropriate to the business requirements for protection and are not unnecessarily strict. The policy therefore must be based upon a clear understanding of the business requirements as specified by the owners of the assets involved. These requirements may depend on factors such as:

- **a)** The security classification of the information stored and processed by a particular system or service.
- **b)** Relevant legislation that may apply e.g. Information Technology Act 2000
- **c)** The regulatory framework in which the organization and the system operates.
- **d)** Contractual obligations to external third parties
- **e)** The threats, vulnerabilities and risks involved
- **f)** The organization's appetite for risk
- **g)** Data protection / privacy regulations as applicable

15.3.3 Business requirements should be established as a part of the requirements gathering stage of new or significantly changed systems and services and should be incorporated in the resulting design.

15.3.4 A warning banner, advising that access to the system is for authorized individuals only, must be shown prior to logging onto all systems and applications classified as CONFIDENTIAL, and, where technically feasible, all other SEFL systems and applications. The warning banner must also reflect local legislation within the subsidiary territory, with regard to penalties for unauthorized access.

15.3.5 In addition to the specific requirements, a number of general principles will be used when designing access controls for SREI's systems and services. These are:

a) Defence in Depth – security should not depend upon any single control but be the sum of a number of complementary controls.

b) Least Privilege – the default approach taken should be to assume that access is not required, rather than to assume that it is.

c) Need to Know – access is only granted to the information required to perform a role and no more.

d) Need to Use – users will only be able to access physical and logical facilities required for their role.

e) The principle of "Identification, Authentication, Authorisation and Accountability" (IAAA) should be implemented at all stages of Access control.

f) Access to applications containing information classified as CONFIDENTIAL or above must be ended automatically after a period of inactivity exceeding 15 minutes, requiring new authentication. Where possible this must be built directly into the application. If this is not possible, secondary authentication, such as password protected screen saver, must be used.

g) Groups of information systems, services and users must be segregated appropriately on the network, e.g. access rights must be provided only to those areas of the network and systems for which they are authorized.

h) Access to shared networks, especially those extending beyond the territory's boundaries should be restricted only to the areas of network segments that the user has authorized access to.

i) Access to system utilities and tools that possess the capability to override the existing security controls must be restricted to a limited number of individuals as dictated by business needs.

15.4 User Access Management

Formal user access control procedures must be documented, implemented and kept up to date for each application and information system to ensure authorised user access and to prevent unauthorised access. They must cover all stages of the life cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access.

All access must be authorized by the Business Department / Information Owner or their delegate who is responsible for the system, application or data.

User access rights must be reviewed at regular intervals – every 180 days or twice a year – by HODs to ensure that the appropriate rights are still allocated. System administration accounts must only be provided to users that are required to perform system administration tasks.

15.4.1 User Registration and De-Registration

A request for access to SREI's network and computer systems must be first submitted to IT Service Desk by relevant authority (HR, Business) for allocation of computer system and creation of user accounts for respective application (i.e. Active Directory, E-Mail, etc.). All requests will be processed according to a formal procedure that ensures that appropriate security checks are carried out and correct authorisation is obtained prior to user account creation. The principle of segregation of duties will apply so that the creation of the user account and the assignment of permissions are performed by different people.

Each user account will have a unique username that is not shared with any other use and is associated with a specific individual i.e., not a role or job title. Generic user accounts i.e. single accounts to be used by a group of people should not be created as they provide insufficient allocation of responsibility. If creation of such account is required, relevant approval process should be followed. Generic privileged accounts (e.g. root) must be used only if unavoidable, with approval from CTO. Under no circumstances must staff user accounts be shared or password information divulged. Staff must be provided with security training on this matter and be advised of the policy when issued with their user account.

An initial strong password should be created on account setup and communicated to the user via secure means. The user must be required to change the password on first use of the account.

When an employee leaves the organisation under normal circumstances, their access to computer systems and data must be suspended at the close of business latest one day after the employee's last working day. It is also the responsibility of the line manager to request the suspension of the access rights via the IT Service Desk. There should be real-time integration between the HRMS and IT systems to achieve this.

In exceptional circumstances where there is perceived to be a risk that the employee may take actions that may harm the organisation prior to or upon termination, a request to remove access may be approved and auctioned in advance of notice of termination being given. This precaution should especially apply in the case where the individual concerned has privileged access rights.

User accounts should be initially suspended or disabled only and not deleted in case of de-registration. User account names should not be reused as this may cause confusion in the event of a later investigation.

15.4.2 User Access Provisioning

Each user must be allocated access rights and permissions to computer systems and data that are commensurate with the tasks they are expected to perform. In general, this should be role-based i.e., a user account will be added to a group that has been created with the access permissions required by that job role.

Group roles should be maintained in line with business requirements and any changes to them should be formally authorised and controlled via the change management process.

Ad-hoc additional permissions should not be granted to user accounts outside of the group role. If such permissions are required, this should be addressed as a change and formally requested.

15.4.3 Removal or Adjustment of Access Rights

Where an adjustment of access rights or permissions is required e.g. due to an individual changing role, this should be carried out as part of the role change, It should be ensured that access rights no longer required as part of the new

role are removed from the user account. In the event that a user is taking on a new role in addition to their existing one, then a new composite role should be requested via change management. Due to consideration of any issues of segregation of duties should be given.

Under no circumstances should administrators be permitted to change their own user accounts or permissions.

15.4.4 Management of Privileged Access Rights

Privileged access rights such as those associated with the administrator level accounts must be identified for each system of network and tightly controlled. In general, technical users should not make day to day use of user accounts with privileged access; rather separate 'admin' user accounts should be created and used only when the additional privileges are required. These accounts should also not be used as they provide insufficient identification of the user.

Access to admin level permissions should only be allocated to individuals whose roles require them and who have received sufficient training to understand the implications of their use.

The use of user accounts with privileged access in automated routines such as batch or interface jobs should be avoided where possible. Where this is unavoidable, the password used should be protected and changed on a regular basis.

Granting of privileged access rights to third party agencies should be avoided as far as possible and if at all given should be with express approval of both CISO and CTO. Such privileged access should be closely monitored, reviewed and withdrawn as soon as the requirement gets over.

15.4.5 User Authentication of External Connections

In line with the network security policy, the user of modem on non-organisation owned PCs or devices connected to SREI's network can seriously compromise the security of the network. Specific approval must be obtained from the IT Service Desk and CISO before connecting any equipment to the organisation's network.

Where remote access to the network is required via VPN, a request must be made via the IT Service Desk. A policy of using two-factor authentications for remote access could be used in line with the principle of something you have and something you know.

15.5 Third Party Access Control Policy and Procedure

15.5.1 Managing Outsourcing and Third Party Access Risks

a) The risks involving external party access to Srei's information and information processing facilities shall be identified and controls implemented before granting access.

b) Third party access to systems must be restricted to the minimum required system level access. The access given should be with express approval of both CISO and CTO. Such privileged access should be closely monitored, reviewed and withdrawn as soon as the requirement gets over.

c) Any external access to Srei's IT systems must follow established procedures.

15.5.2 Contractual Issues

a) All third parties given access to Srei's IT systems must agree to abide by Srei's information security policies prior to being granted access.

b) Srei will assess the risk to its information and, where deemed appropriate because of the confidentiality, sensitivity or value of the information being disclosed or made accessible, Srei will require third party suppliers of services to sign a confidentiality agreement to protect its information assets.

c) Where relevant, third parties should be asked to provide a copy of their information security policies.

d) All contracts with external suppliers for the supply of services to Srei must be monitored and reviewed to ensure that information security requirements are being satisfied.

e) Contracts must include appropriate provisions to ensure the continued security of information and systems in the event that a contract is terminated or transferred to another supplier.

f) The Service Level Agreement (SLA) should be approved by Legal Department and should contain provisions for Data Protection & Privacy as laid down by regulators and Government from time to time. The penalty clauses should protect SREI from all potential losses and damages, including reputation loss.

g) The SLA should contain clauses enabling SREI to conduct Information Security Audit of vendor IT systems.

15.5.3 Third Party Support and Maintenance

a) Srei staff must not permit information security safeguards to be bypassed, or allow inappropriate levels of access to the Srei information or IT facilities to any third parties.

b) Persons responsible for agreeing to maintenance and support contracts will ensure that contracts being signed are in accordance with the Srei's information security policies.

15.5.4 Facilities Management and Outsourcing

Any facilities management (such as PC maintenance) outsourcing company with which Srei may do business must be able to demonstrate compliance with Srei's information security policies and enter into binding service level agreements that specify the performance to be delivered and the remedies available in case of non-compliance.

15.5.5 Physical Access by External Parties to Sensitive Areas

A risk assessment must be conducted and appropriate controls established before granting third party access to secure areas where confidential information is stored or processed. This also applies to secure areas containing active network equipment.

15.5.6 Electronic Remote Access by External Parties

Remote access by External Parties to the Srei network must be limited to the minimum required system level access. Any request for access must first be approved by the CTO / CISO or their nominated deputy. All protection measures as laid down in the Cyber Security policy should be adhered without fail.

15.6 Mobile Computing & Remote Access

15.6.1 Scope

Employees, Consultants, Vendors, Contractors and others who are using mobile computing and storage devices on the network at Srei are in the purview of this policy.

15.6.2 List of default services remotely available to Srei users

Currently, the following services are available to Srei employees from anywhere:

a) Google mail for Srei domain

b) Employwise

c) Srei VPN

15.6.3 Policy

Mobile computing and storage devices containing or accessing the information resources at Srei must be approved prior to connecting to the information systems at Srei. This pertains to all devices connecting to the network at Srei, regardless of ownership. Mobile computing and storage devices include, but are not limited to: laptops, personal digital assistants (PDAs), plug-ins, Universal Serial Bus (USB) port devices, Compact Discs (CDs), Digital Versatile Discs (DVDs), flash drives, cloud storages, modems, handheld wireless devices, wireless networking cards, and any other existing or future mobile computing or storage device, either personally owned or owned, that may connect to or access the information systems at Srei. A risk analysis for each new media type shall be conducted and documented prior to its use or connection to the network at Srei unless the media type has already been approved by the Information & Cyber Security Team.

15.6.4 Roles & Responsibilities

Users of mobile computing and storage devices must diligently protect such devices from loss of equipment and disclosure of private information belonging to or maintained by Srei. Before connecting a mobile computing or storage device to the network at Srei, users must ensure it is on the list of approved devices issued by the Information & Cyber Security Team. The Enterprise Help Desk must be notified immediately upon detection of a security incident, especially when a mobile device may have been lost or stolen. The Information Security (InfoSec) Team is responsible for the mobile device policy at Srei and shall conduct a risk analysis to document safeguards for each media type to be used on the network or on equipment owned by Srei.

SREI shall endeavor to:

a) Implement a Network Access Control (NAC) solution to protect the interest of the organization.
b) Email security solution for protecting organizational IT assets.

15.7 Review of User Access Rights

15.7.1 On a regular basis asset and system owners will be required to review who has access to their areas of responsibility and the level of access in place. This is to identify:

a) People who should not have access

b) User accounts with more access than required by the roles

c) User accounts with incorrect role allocations

d) User accounts that do not provide adequate identification e.g. generic accounts

e) Access rights given to external / third parties

f) Regular review of privileged access given to internal / external parties

g) Any other issues that do not comply with the policy

15.7.2 This review will be performed according to a formal procedure and any corrective actions identified and carried out.

15.7.3 A review of user accounts with privileged access will be carried out on a quarterly basis to ensure that this policy is being complied with.

15.8 User Authentication and Password Policy

15.8.1 A strong password is an essential barrier against unauthorized access. Unfortunately, this area is often proven to be the weak link in an organisation's security strategy and a variety of ways to improve the security of user authentication are available, including various forms of two factor authentication and biometrics.

15.8.2 SREI's policy is to make use of additional authentication methods based on a risk assessment which takes into account:

- **a)** The value of protected assets
- **b)** The degree of threats believed to be existing
- **c)** The cost of the additional authentication methods
- **d)** The ease of use and practicality of the proposed methods
- **e)** Any other relevant controls in place

15.8.3 Use of multi-factor authentication methods should be justified on the basis of the above factors and securely implemented and maintained where appropriate.

15.8.4 Single Sign On could be used within the internal network where supported by relevant systems unless the security requirements are deemed to be such that a further login is required.

15.8.5 Whether single or multi factor authentication is used, the quality of user passwords should be enforced in all networks and systems using following parameters.

15.9 System and Application Access Control

15.9.1 As part of the evaluation process for new or significantly changed systems, requirements for effective access control should be addressed and appropriate measures implemented.

15.9.2 These should consist of a comprehensive security model that includes support for the following:

- **a)** Creation of individual user accounts
- **b)** Definition of roles or groups to which user accounts can be assigned
- **c)** Allocation of permissions to objects of different types to subjects
- **d)** Implementation of Maker-Checker principle of authorization to reduce the risk of error and to ensure reliability of information
- **e)** Provision of varying views of menu options and data according to the user account and its permission levels.
- **f)** User account administration, including ability to disable and delete accounts.
- **g)** User login controls such as:
    - **i.** Non display of password as it is entered.
    - **ii.** Account lockout once number of incorrect login attempts exceeds a threshold
    - **iii.** Provide information about the number of unsuccessful login attempts and last successful login.
    - **iv.** Date and time based login restrictions

v. Device and location based login restrictions

h) User inactivity timeout

i) Password management including:

i. Ability for user to change password

ii. Controls over acceptable passwords

iii. Password expiry

iv. Hashed / encrypted password storage and transmission

j) Security auditing facilities, including login / logout and unsuccessful login attempts.

15.9.3 Where software development is undertaken, program source code should be protected from unauthorized access in accordance with industry best practices.

15.9.4 Access to utility programs that provide a method of bypassing system security (e.g. Data manipulation tools) should not be permitted. Any exception should be approved by CTO and CISO.

15.10 User Responsibilities

15.10.1 The security of information depends upon the degree of care exercised by the users of networks and systems in their day to day roles. Many recent high profile security breaches have been largely caused by unauthorized access to user accounts resulting from passwords being stolen or guessed.

15.10.2 It is therefore vital that every user plays his or her part in protecting the access they have been granted and ensuring that their account is not used to harm the organisation.

15.10.3 In order to maximise the security of information, every user must:

a) Use a strong password i.e. one which is in line with the rules as per the password policy

b) Never reveal their password or allow anyone else to use their account

c) Not record the password in writing or electronically e.g. in a file or email

d) Avoid using the same password for other user accounts, either personal or business related

e) Ensure that any PC or device they leave unattended connected to the network is locked or logged out

f) Leave nothing on display that may contain access information such as login names and passwords

g) Inform the IT Service Desk of any changes to their roles and access requirements.

15.10.4 Failure to comply with these requirements may result in the organisation taking disciplinary action against the individual concerned.

16. Cryptography

16.1 Key Control Objective

The implementation of cryptographic controls over Srei information systems will help in protecting the confidentiality, integrity and authenticity of the information.

16.2 Private Key Protection Controls

16.2.1 Key Pair Generation and Installation

a) Both for Public and Private

b) Generation of Certificate Signing Request (CSR) using the private key and sharing the CSR files to the CA for certificate (Srei doesn't share the private key to the CA vendor)

16.2.2 Private Key Multi-Person Control: Single person is dedicated to install the keys as maker and another person is there to keep in his / her custody as checker.

16.2.3 Private Key Back-up: The file is kept in a secure folder within the organization, restricted among the maker and checker users

16.2.4 Method of Activating Private Key

a) Certificate file

b) Need to provide the private key and;

c) Intermediate certificate to be generated by the vendor

16.2.5 Security Services Method: Information & Cyber Security Team will periodically review the list of key security service areas (existing and upcoming) and suggest if any new action / change needs to be incorporated in the current policy and procedures.

16.2.6 Method of Deactivating Private Key: It is completely need based (in the case of lost or old keys)

16.2.7 Monthly review of Private Key: Monthly review should be conducted to ensure that the respective stakeholders are adhering to the policy. Deviations need to be captured and documented with proper reason.

17. Physical and Environmental Security

17.1 Key Control Objective

Appropriate security controls must be put in place within Srei premises to protect against the risk of theft or unauthorized access to Srei information and technology assets.

17.2 Controls

17.2.1 The security perimeters for Srei buildings must be well defined and physically sound. External doors of Srei areas must be suitably protected against unauthorized access.

17.2.2 Reception areas must be manned by either a receptionist(s) or security guard(s). All building visitors shall be appropriately logged when entering the building. With the exception of publicly accessible / open areas, all visitors must be escorted by a member of staff, not including those third party contractors who have been screened and granted an access pass to the Srei building.

17.2.3 All staff must be issued a staff identification card, with photograph where legally permissible, that must be worn visibly at all times around the neck with lanyard and checked when entering Srei premises. Vendors / contractors, who are deputed at company premises, must be identifiable by way of different coloured lanyard; in addition, they shall also wear their own organization-provided identity cards while on duty within Srei premises.

17.2.4 Visitors to Srei must be issued Visitor ID cards with different coloured lanyard which must be worn by them within premises.

17.2.5 Access to areas hosting information classified as CONFIDENTIAL or information processing centres must be restricted only to staff who are authorized to have access to those areas. Such areas must be situated away from public areas. Access must be controlled through appropriate electro-mechanical access control system. In addition, audit control logs, detailing access, must be periodically reviewed and stored for a minimum period of 90 days.

17.2.6 Vendors or visitors requiring access to secure areas, such as information processing centres, who have not been vetted using the standard Srei staff vetting procedures, must be escorted at all times by an authorized member of staff. In addition, their access must be recorded in a visitor/vendor tracking book and be pre-authorized by a relevant member of staff.

17.2.7 All external access doors, including fire doors, must close and open effectively. They must never be propped open unless continuously monitored by a staff member or authorized security personnel.

17.2.8 Specific areas such as server rooms, information processing facilities, and certain offices depending on their criticality and risk exposure, should be categorized as ‘secure areas’ and appropriate controls should be implemented. Such secure areas should have additional controls implemented including, but not limited to the following:

a) Vacant secure areas should be locked and periodically checked;

b) Unsupervised working in the secure areas should be avoided, both for health and safety reasons, and to prevent any potential malicious activities.

17.2.9 A clear-desk policy must be enforced throughout the organization. Documents and other information that is classified as CONFIDENTIAL or above must be locked away when not in use, especially outside office hours. Such documents may also be shredded.

17.2.10 Documents and information classified as CONFIDENTIAL must be stored in a fire-protected safe or cabinet for which access must be limited only to authorized personnel.

17.2.11 Photography is not allowed within office premises, unless authorized by HR/Admin.

17.2.12 Physical protection against damage from natural or man-made disasters such as fire, flood, earthquake, explosion and civil unrest that are appropriate to the location shall be developed and implemented appropriately.

17.2.13 Smoking is banned within office premises.

17.2.14 Access entry points such as delivery and loading areas shall be controlled in an appropriate manner and where needed and possible, such areas shall be isolated from secure areas to avoid unauthorized access.

17.2.15 Only staff and authorized vendors' vehicles are allowed inside.

17.2 16 Equipment shall be placed and hosted in a secure manner, to minimize the risks from environmental threats and hazards.

17.2.17 Critical equipment shall be protected against any potential loss of power supply and other disruptions that may be caused by the failure of any supporting utilities.

17.2.18 Power and telecommunication cables supporting information services or carrying data shall be secured against unauthorized access or damage.

17.2.19 Equipment shall be maintained properly to ensure their continual availability. They should be serviced at regular intervals and as stipulated by any SLAs and insurance contracts.

17.2.20 All equipment, including media containing CONFIDENTIAL or TOP SECRET information, shipped out of their primary location should be protected both whilst in-transit and when housed at any external location. Insurance arrangements should provide cover for equipment stored and used at offsite locations. Equipment should not be moved off-site without proper authorization.

17.2.21 All equipment or storage media should be checked for the existence of any sensitive data and licensed software, and such data and software shall be securely removed or securely overwritten prior to the disposal or destruction of such equipment or media.

17.2.22 Biometrics: Biometrics is a technology for measuring and analyzing biological data of a human body such as fingerprints, eye retinas, irises, voice patterns, facial patterns, and hand geometry, and vascular patterns and DNA. Biometrics is mainly used for authentication purposes. Biometrics technology is used to prevent fraud, enhance security and reduce identify theft. Biometric access control to be introduced at user end points which involves:

a) Log on to IT systems

b) Acquiring data

c) Extraction of features

d) Access is allowed or denied based on the match or no-match.

17.2.23 Interception of data:

a) Data cables running within the organization, particularly in infrequently used areas, should be completely concealed so that they cannot be tampered with and to avoid the possibility of anybody fixing a monitoring / sniffing device to them. Data cables running outside the organization should be completely concealed and should be well-protected so that there is no possibility of tampering by anybody.

b) In case of wireless devices, it should be seen that there is hardly any possibility of anybody using any rogue wireless router from outside the perimeter of the organization. The communication from the wireless devices need to be encrypted through a strong encryption mechanism so that they are not interfered with and tampered with.

c) LAN points should not be normally provided in the visitor area or discussion rooms where the visitors are allowed so that there is no possibility of any visitors connecting to the LAN and manipulating the network.

17.2.24 Intrusion Detection

a) Intrusion Prevention System (IPS) should be deployed to protect organisational IT assets.

b) Network Access Control (NAC) and Data Leak prevention (DLP) solutions should be deployed on all critical IT assets / networks.

18. Operations Security

18.1 Key Control Objective

To ensure correct and secure operations of information processing facilities, it is vital that proper security controls are applied within all Srei information processing centres.

18.2 Controls

18.2.1 Formal operating procedures must be documented for the information processing centre and be approved by CTO. These procedures must be made available to all relevant users on a need-to-know basis.

18.2.2 Formal change management procedures that provide a consistent approach to initiate, execute and manage changes to the operating environment must be developed and implemented.

18.2.3 All system documentation (e.g., operating procedures, patch management, architecture diagrams and router configurations) must be stored in a secure location (e.g. fire protected safe/offsite storage facility).

18.2.4 To ensure the availability of the operating environment and network services, capacity planning must be conducted prior to any significant changes to the operating environment that may impact on its operability and availability. Periodic incremental reviews should be conducted to ensure service operating and availability levels are maintained.

18.2.5 Appropriate segregation must exist between production and testing environment. All development changes must be properly tested in a logically and physically separate environment, and test results documented. The testing environment must be designed so that any issues within the test environment will not impact the production environment. All development changes must be authorized through change management procedures (e.g., acceptance criteria, Information Owner sign-off) prior to transfer to the production environment.

18.2.6 Controls should be put in place to detect, prevent and recover systems from malicious activity such as unauthorized access, viruses, spyware and Trojans. Controls include, but are not limited to, software to detect and prevent/remove malicious activity such as antivirus, personal firewall and anti-spyware. This software must be updated with the latest signature and detection files on a scheduled basis, and within 72 hours of solution becoming available, when critical or high risk vulnerabilities are identified. Automatic virus and malicious software scanning checks must be carried out on all electronic attachments and files that are received from external sources. In addition, systems must be configured to perform on either a complete system scan on a weekly basis (minimum), or permanent on-access scans.

18.2.7 USB mass storage is disabled by default on all systems. Exceptions need approval of HOD, CTO and CISO with adequate business justification and the time till which it has to be enabled for such requirement, before it can be processed; such approvals are valid for bare minimum required period only.

18.2.8 Data must be backed up in accordance with the requirements specified by the information owners. Operational procedures must verify the successful completion of backups. Backed-up data must be stored in a secure location both within Srei and when stored at an off-site location. Back-up tapes must be clearly identifiable. The offsite location used for storing back-up tapes must be of a distance close enough to ensure the availability of the tapes in the event of a disaster at the Srei site but far enough not to be compromised by the likelihood of disasters in the area. Procedures must be put in place to ensure back-up media will operate in the event of an emergency.

18.2.9 Enable audit trail & logs must be created for all security related activities in all systems, database, network and applications for review, audit trail and forensic investigation purpose. Audit trails to be reviewed regularly for anomalies.

18.2.10 Faults that are reported must be logged together with corrective action taken; procedures must be put in place to review these logs to ensure that faults have been appropriately resolved within applicable timeframes, such as those imposed by legal, regulatory or contractual requirements.

18.2.11 End users should not be able to change their system time by themselves, to protect the manipulation of information required during incident handling and analysis. Only authorized requests for correction of system time should be handled by appropriate help desk personnel with administrative access and logs should be available to record and analyse such incidents.

18.2.12 Date and time accuracy that supports audit logging must be ensured by synchronizing all system clocks to a single reliable time source and checked periodically. A formal change control procedure must be followed for all changes made to any operational system. Only authorised changes must be applied to operational systems by authorised person.

18.2.13 Vulnerability Assessment scanning should be conducted on regular intervals. This will ensure information about technical vulnerabilities of information systems being used by Srei and the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.

18.2.14 Users must not have administrative privileges on their local system. This will ensure restriction on installation of unauthorised software on operational systems. Regular system audit will ensure software compliance and will help identify and remove unauthorised software from operational systems.

18.2.15 CTO and CISO will be jointly responsible for ensuring Operational Security of IT operations in the organisation.

18.2.16 Security Operations Centre (SOC) – There shall have a dedicated 24X7 Security Operations Centre (SOC), either to be maintained internally or outsourced, for monitoring of security events to detect and rapidly respond to cyber-attacks on production (DC) network, application and infrastructure.

- **a)** Data Loss Prevention measures, spanning from endpoint to servers and from e-mails to smartphones.
- **b)** Implementation of Mobile Device Management.
- **c)** LAN segmentation, NAC (Network Access Control), VPN (Virtual Private Network), endpoints hardening, encryption of data at rest, in use and in motion, protection through well configured and monitored IPSs / IDSs, firewalls, routers and switches.
- **d)** To build a complete technological environment: firewalls, Web Application Firewalls (WAF), IPSs / IDSs, breach detection solutions, probes and obviously a SIEM.

19. Clear Desk Policy

19.1 All sensitive information should be kept in a secure place in office or other location e.g. storage in a locked drawer, file cabinet etc.

19.2 All non-public documents when printed or scanned should be cleared from printers or scanners immediately.

19.3 All incoming and outgoing mail points and unattended facsimile machines should be protected from unauthorized physical and logical access.

19.4 Unauthorized use of photocopier and other technologies which can duplicate (e.g. scanners, digital cameras etc.) should be prevented.

19.5 Where practically possible, paper and computer media should be stored in suitable locked safes, cabinets or other forms of security furniture when not in use, especially outside working hours.

19.6 Sensitive or classified information, when printed, should be cleared from printers immediately.

19.7 Confidential or sensitive information should not be held on the desk within reach/sight of visitors.

19.8 Any unattended printouts, fax available on the desk should be cleared by end of the day.

20. Clear Screen Policy

20.1 Personal computers, computer terminals and printers should be left logged off or protected with a screen and keyboard locking mechanism controlled by a password or similar user authentication mechanism when unattended.

20.2 The maximum time to activate screen savers is 15 minutes of user inactivity with the system getting locked.

20.3 Time duration to activate password protected screen savers is dependent on the locations and this should be activated within 5 minutes of user inactivity.

20.4 The maximum session timeout for the applications internally is 15 minutes.

20.5 Users should log off or lock their personal computers when leaving it unattended for any period of time.

21. Network Management Policy

21.1 Intent

The purpose of this policy is to assure Confidentiality, Integrity and Availability of Network Infrastructure at Srei Group Companies (hereinafter referred to as “Srei”). This network documentation policy is an internal policy.

21.2 Objective

21.2.1 Organization’s investment in Network should be leveraged to ensure customer orientation, reducing costs and improve operational efficiency by ensuring the availability, scalability and superior performance of its network. The policy should facilitate following business requirements:

- **a)** To facilitate networked financial operations using technological solutions suitable for business.
- **b)** To allow for business continuity during network disruptions by providing at least one backup link at networked locations.
- **c)** To provide need based network access to different networked locations.
- **d)** To integrate with external networks required for conduct of Business

21.2.2 This policy should complement disaster management and recovery by ensuring that documentation is available in the event that systems should need to be rebuilt.

21.2.3 This policy will help reduce troubleshooting time by ensuring that appropriate personnel are notified when changes are made to the network.

21.3 Scope

This policy applies to the access and usage of network services and entire Network Infrastructure of Srei.

21.4 Applicability

This policy applies to SREI Information Technology Department & Support Partner (If any) who is responsible for designing, implementing, configuring, managing and maintaining and protecting Srei’s Network Infrastructure.

21.5 Policy Statements

21.5.1 Documentation

The Network Infrastructure configuration shall be documented and provide the following information:

- **a)** IP addresses and host names of all network devices with public and private IP addresses as applicable.
- **b)** Complete inventory of DHCP Pool.
- **c)** Inventory of Public Routable IP Address obtained from Internet Service Provider(s)
- **d)** Detailed configuration documentation including but not limited to Source, Destination, Ports, Protocols, Services and Business justification for the same
- **e)** High level and detailed network diagram.
- **f)** Network diagrams should have the following but not restricted to -
    - **i.** The location, hostname and IP addresses of all hubs, switches, routers, firewalls, IPS and other network devices on the network
    - **ii.** Site to site interconnectivity using MPLS or P2P or IPsec VPN tunnel or any other technology and the associated switch / firewall and port on the switch / firewall supplying that connection

iii. The interrelationship and or interconnectivity between all network devices showing connectivity lines running between the network devices

iv. All subnets on the network and their relationships including the range of IP addresses on all subnets and netmask information

v. All wide area network (WAN) information including network devices terminating them and IP addresses of connecting devices

vi. Wireless Networks and access points

vii. DMZ

g) Configuration information of all network devices including (but not restricted to):

i. Switches

ii. Routers

iii. Firewalls

iv. DHCP Server

v. Radius / TACACS Server

vi. Wireless Access Point

vii. IPS/IDS device

h) Network connection information including (but not restricted to):

i. Type of connection to the Internet or other WAN/MAN including MPLS, P2P Link, IPsec VPN

ii. Provider of Internet/WAN/P2P connection and contact information for sales and support

iii. Configuration information including IP address, netmask, network ID, and gateway

iv. Physical location of where the cabling enters the building and circuit number

21.5.2 Configuration

a) The Confidentiality, Integrity, Availability, Security, and proper operation of the Srei network require an orderly assignment of network addresses and the correct configuration of devices attached to the network.

b) Network access, performance, and security are put at risk when devices are introduced into the network environment without appropriate configuration.

c) Any departments and individual users may not install, alter, extend or re-transmit network services in any way.

d) Departments and individual users are prohibited from attaching or contracting with a vendor to attach equipment such as routers, switches, hubs, firewall appliances, wireless access points, proxy servers and any other network or server device to the Srei network without prior authorization from Srei IT.

e) Personal device are also not permitted to connect to the Srei network without explicit approval from CTO citing proper business justification and need for the same.

The network configuration must consider but not limited to following points:

21.6 Local Area Network

21.6.1 LAN must apply controls to protect data passing over the network and prevent unauthorized access

21.6.2 LAN is segregated with different VLAN to reduce broadcast in the network

21.6.3 No individual is permitted to connect any personal network equipment in SREI network without explicit approval from CTO citing proper business justification and need for the same.

21.6.4 IP addressing should be DHCP enabled. Where ever DHCP is not available Static Manual IP addressing can be used.

21.7 Wide Area Network

21.7.1 All RO and Branch network is connected with MPLS network.

21.7.2 Branch locations where MPLS network is not available should connect to Srei network via corporate VPN.

21.8 Network Redundancy

21.8.1 Adequate redundancy should be provided for critical network links. The level of redundancy should depend on the criticality of applications utilizing the link. For critical links, including inter-office WAN connections, there should be redundant link configured with automatic failover to ensure that there is minimum disruption of business.

21.8.2 Redundant links should have the same level of security as the primary links.

21.8.3 If the primary link offers encryption and firewall protection, the secondary link should also have similar security level.

21.8.4 Redundant link should be checked periodically for normal working and automatic switchover.

21.8.5 Redundant network devices should be installed in failover or load balancing mode based on the criticality of applications being supported by the network devices.

21.9 Network device configuration guide

21.9.1 Management Access:

Telnet may never be used across any network to manage a router or switch, unless there is a secure tunnel protecting the entire communication path. SSH version 2 and above or https is the preferred management protocol.

21.9.2 User Access Management:

a) Session lockout threshold 5 failed loggin attempts
b) Lockout duration is one minute
c) Session time out 15 minutes
d) No system default user accounts and passwords should be enabled.
e) No Generic user accounts should be created or used.

21.9.3 Password Management:

All router and switches should have secret password enabled. Clear text passwords should not be allowed. All network equipment password should be at least 8 character long, alphanumeric with special character.

The below mentioned points also needs to be considered but not limited to -

a) Password history – 3 passwords remembered.
b) Password age – 60 days
c) Password expiry warning – 14 days
d) All vendor supplied default passwords should be changed.

21.9.4 Service Configuration Restriction:

The following services or features must be disabled on:

a) IP directed broadcasts

b) Incoming packets at the router/switch sourced with invalid addresses such as RFC1918 addresses

c) TCP small services

d) UDP small services

e) All source routing and switching

f) All web services which is running on router

g) Cisco discovery protocol on Internet connected interfaces

h) Telnet, FTP, SMTP, POP3 and other clear text protocol services.

i) Auto-configuration

21.9.4 NTP Configuration: All network devices should sync time from Local NTP Server which will sync time from global stratum.

21.9.5 SNMP Configuration: Don't use default SNMP community strings. Use SNMP version 3.

Default strings, such as public or private must be removed. SNMP must be configured to use the most secure version of the protocol allowed for by the combination of the device and management systems.

21.9.6 Use of IPv6 platform should be enabled as per National Telecom Policy issued by the Government of India in 2012.

21.9.7 Login Banner: Each router must have an approved pre and post login banner statement presented for all forms of login whether remote or local.

21.9.8 Audit Trail and Syslog: Enable audit trail and syslog in all network equipment's (Router, Switch, Firewall IPS, Wireless AP and others) for review, audit and forensic investigation purpose. System and Security logs should be stored for a minimum period of 90 days.

21.9.9 Corporate Wi-Fi Network

a) Use radius authentication in all access point device

b) Use MAC binding and AD authentication for all end user devices

c) Use WPA 2 Enterprise as Wireless Security Protocol.

d) Use AES as the encryption algorithm

e) Do not use WEP as Wireless Security Protocol.

f) User will get dynamic IP address from DHCP Server.

21.9.10 Visitor Wi-Fi Network

a) Visitor Wi-Fi Network / Access Point should be segregated from Corporate Wi-Fi Network.

b) Segregation of Visitor Wi-Fi Network and Corporate Wi-Fi Network to be done through Firewall.

c) Web Access Restriction is configured on firewall

d) Guest user will get dynamic IP address from Firewall DHCP pool.

e) All Visitor Wi-Fi Access passphrase to be changed after every 7 days.

f) Wi-Fi Access Key / Passphrase to be generated through Key generator.

21.9.11 Firewall Policy Configuration

a) Only port base access is allowed from inside to outside network and outside to inside network.

b) Only port base access are allowed from Edge VPC (DMZ) to Private VPC (MZ)

c) All port access can allow MZ to DMZ MAKE SAME CHANGE

d) On-prem (LAN) to Edge VPC (DMZ) access is allowed after provide the proper justification and necessary approval.

e) Session Logging needs to enabled in all policy

f) Firewall web filter needs to enabled at all internet access policy

21.10 VPN Configuration guide

21.10.1 SSL VPN Configuration Guide

a) Enable tunneling mode with split tunneling

b) For Remote Access VPN allow access per business justification and role based.

c) Encryption algorithm settings should be High-AES and 3DES (128/256 bits)

d) Two factor authentications should be enabled.

e) Only AD authenticated users can access SSL VPN

21.10.2 IPsec VPN Configuration Guide

a) Preshared key should be atleast 8 character in length, alphanumeric with special character.

b) Encryption type AES / 3 DES 128- 256 BIT

c) Authentication SHA 2 and above

d) DH Group 2

e) Keylife 86400 sec.

f) Pre-shared key at both tunnel ends to be changed at least once in 6 months.

21.11 Device management

21.11.1 No individual is permitted to independently deploy network devices that extend the Srei network

21.11.2 Only authorized person can do necessary changes or modification in Srei network.

21.12 Update & Communication

IT Operations Team, IT Application Team, IT Helpdesk and the Information & Cyber Security Team shall be notified when network changes are made including:

21.12.1 Reboot of a network device including switches, routers, and firewall

21.12.2 Changes of rules or configuration of a network device including switches, routers, and firewalls

21.12.3 Upgrades to any software / Firmware on any network device

21.12.4 Additions of any software / Firmware on any network device

21.12.5 Changes to any servers which perform significant network functions whether configuration or upgrade changes are made. These servers include:

a) DHCP

b) Radius

c) Proxy

d) AD

e) Antivirus

f) WSUS

21.12.6 Notification shall be through email to designated groups of people.

21.13 Network protection

21.13.1 Devices posing an immediate threat to the Srei network will be disconnected from the network to isolate the intrusion or problem and minimize risk to other systems until the device is repaired and the threat is removed.

21.13.2 Devices involved in repeated incidents may be disconnected from the Srei network for longer periods of time as required to reduce security risks to an acceptable and sustainable level. Server administrators will be required to demonstrate compliance with Server Management Policy, and security standards and procedures through an audit review or other assessment of the network attached devices for which they are responsible.

21.13.3 IT Operations will adhere to all applicable rules of 'network security policy' to ensure confidentially, integrity & availability of network is maintained to the highest possible level.

21.13.4 NAC solution to be implemented to effectively manage devices connected to the network.

21.14 Network access policy

21.14.2 Internet access

Users can access internet through authenticated proxy and common internet gateway. For details, refer to Web Access & DLP (Data Loss Prevention) Procedure.

21.14.3 Applications and Server access

- **a)** All applications are located centrally and branch and remote users access applications via WAN / MPLS
- **b)** Internet facing servers should be installed in Demilitarized Zone (DMZ) protected by Intrusion prevention Systems and Web Application Firewalls.
- **c)** All intranet applications, servers and database servers will be installed in Militarized Zone (MZ)
- **d)** WAF must be placed before web server.
- **e)** Database for the web application should host in a separate server, especially for externally exposed applications.
- **f)** The web server and database server must be separated by a firewall with limited port and application specific access.
- **g)** Communication must be encrypted between client and web server, database server.

21.14.4 Remote access

Refer to VPN Usage and Access Policy for details.

21.15 Access control

21.15.1 Group or common access is not allowed for network equipment

21.15.2 Individual login credential needs to configured to access network equipment

21.15.3 Role based Access control mechanism based on "least privilege" should be followed.

21.15.4 "Deny All" settings to be enabled by default in all network devices. Access to be allowed with proper business justification and role based.

21.15.5 Physical and logical access to diagnostic and configuration ports must be restricted.

21.15.6 Routing controls must be implemented to ensure that computer connectivity and information flows do not breach the access controls implemented on the applications.

21.16 Network access for POC / UAT

21.16.1 POC/UAT network environment should be different from production environment

21.16.2 Require port, protocol and service details before go live into production environment

21.16.3 If POC/UAT application is required to communicate with production environment, then communication should happen on identified / specific port with defined source and destination address.

21.16.4 There should be per identified time line for POC / UAT to communicate with production environment.

22. Communications Security

22.1 Key Control Objective

The key objective is to ensure the protection of information in networks and its supporting information processing facilities.

22.2 Controls

22.2.1 All external network perimeters must be hardened and configured to protect against unauthorized traffic. All inbound and outbound points must be protected by means of firewalls and intrusion detection systems (IDS) or intrusion prevention systems (IPS) with procedures for review of all firewall logs and processes for investigating IDS/IPS alerts.

22.2.2 A Virtual Private Networking (VPN) device or equivalent must be used when company PCs connect remotely to the internal Srei network to set up an encrypted communications tunnel with appropriate logging and monitoring controls.

22.2.3 External third parties must only access the Srei internal network through Srei VPN or equivalent encrypted channel that meets standards defined by Srei.

22.2.4 All wireless networking must provide a level of security that is of a level commensurate to the security that is provided by the external perimeter networks.

22.2.5 Perimeter assets must only be accessed by authorized staff and such access must only occur through secure and approved management ports.

22.2.6 Controls must be put in place, within the network, to ensure that unauthorized activity is identified. Controls must also ensure that services levels perform at an optimum, and that data which is passed across the network is secure.

22.2.7 An appropriate disclaimer(s) must be assigned to e-mails that are sent outside the company in accordance with appropriate legislation within Srei. Non-business e-mails, sent using the company's Lotus Notes, must be flagged and indicate that the e-mail is not sent on behalf of Srei.

22.2.8 All incoming and outgoing electronic mail must be scanned to check for viruses, malicious code, file attachments (where legally permissible) and messages that originate from inappropriate sites or email servers.

22.2.9 While in Srei office/network, user shall connect to Internet only through corporate proxy/firewall/other IT designated means and not by any other means like dialup, wireless connection of neighbouring office, etc. Use of Internet data cards must be restricted to connectivity requirements while travelling or in absence of Srei LAN connectivity at home, Srei meeting room or any non Srei location.

22.2.10 Requirements for confidentiality or non-disclosure agreements reflecting the Srei's needs for the protection of information shall be identified, regularly reviewed and documented.

22.2.11 All electronic communications that are accessed, created, sent, received, transmitted, stored, or processed on Company IT assets, whether personal or business, and whether in final, draft, or deleted form, are not considered private, despite any contrary designation. The Company reserves the right to monitor, access, edit,

discard, preserve, divert, divulge and otherwise manage or use all electronic communications on Company IT assets, whether personal or business, and whether in final, draft, or deleted form, at any time and without notice in order to respond to subpoenas and court orders, to otherwise comply with the law, to investigate complaints and allegations, to prevent harassing or threatening messages, to enforce this Policy, to enforce other policies of the Company, for security checks, for maintenance purposes, or as the Company otherwise determines is necessary in its sole determination. Additionally, public websites, including social media sites, are subject to monitoring by the Company at any time and without notice. The Company may take possession of and search any Company devices or authorized devices used to access Company IT systems or generate Company electronic communications in order to facilitate such rights, and any user who fails to comply with a request by the Company for such search will be deemed in violation of this policy. If possible illegal activity is detected, electronic communications that are accessed, created, sent, received, transmitted, stored, or processed on Company IT assets or authorized devices may be provided to law enforcement.

22.2.12 Users may not intercept or disclose, or assist in intercepting or disclosing, electronic communications of another user that are accessed, created, sent, received, transmitted, stored, or processed on Company IT assets unless specifically authorized by the Company or such other user.

22.2.13 Ensure the usage of digital signatures to protect the authenticity and integrity of important electronic documents (wherever applicable).

22.2.14 Electronic Communications Content: The following standards apply to all Electronic Communications accessed, created, sent, received, transmitted, stored, or processed on Company IT assets, whether personal or business, and all Company electronic communications.

22.2.15 The electronic communication must not violate any law.

22.2.16 Users should exercise professionalism and judgment, and take the most prudent action possible, complying with this and all other Company policies including, for example, the Standards of Business Ethics, the Company's solicitation and distribution policy and the Company's policy against harassment and discrimination. Electronic communications should never contain any defamatory, sexually oriented, obscene, harassing, threatening, illegal or fraudulent language.

22.2.17 The Company logo and trademarks may not be used in any form without explicit prior permission in writing from the communications department, unless otherwise permitted by law.

22.2.18 Users must comply with policies related to confidentiality, non-disclosure, privileged information and intellectual property protections such as copyright, trademark and fair use laws.

22.2.19 Guidelines on usage of social media platforms

a) Using work-related social media - Only the corporate communication team is permitted to post material on a social media website in the company's name and behalf. Anyone who breaches this restriction will be subject to the company's disciplinary procedure.

b) Every time when a new social profile is created for / on behalf of SREI, the Corporate Communication Team should perform adequate Risk assessment or ensure go-ahead from the Information & Cyber Security Team so that all the risk associated with the new profile are mitigated / addressed accordingly.

c) Approved social media profile / websites for Srei are Facebook, YouTube, Twitter and LinkedIn. This list may be updated by the Corporate Communication team as per the business requirements. The Corporate Communication team must document & periodically review the Social media presence as part of their process note

d) Before using work-related social media, the users must:

i. Read and understood the corporate communication policy and

ii. Seek and gain prior written approval to do so from the corporate communication team

e) The roles and functions which will be needed moving forward have been identified as follows:

i. Tweeting corporate news – Corporate Communication Team

ii. Advertising promotions on Facebook, YouTube, Twitter and LinkedIn – Corporate Communication Team

f) Any employee involved in the organisation's social media activities must remember that they are representing the organisation, use the same precautions as they would with any other communication and adhere to the following rules:

i. Ensure that the purpose and benefit for the organisation is clear;

ii. Obtain permission from a manager before using social media; and

iii. Ensure the content is checked before it is published

g) The stakeholder (Corp team) should ensure that in case of any IT security / cyber security event or incident occurs, same needs to be informed to Incident manager and CISO on priority and accordingly RCA/information should be submitted by stakeholder in the pre-defined format of reporting

22.2.20 Using personal social media – Personal use of social media in the workplace is permitted, subject to certain conditions, as detailed below;

a) It must not be abused or overused and the company reserves the right to withdraw permission at any time;

b) It must not involve unprofessional or inappropriate content;

c) It should not interfere with employee's responsibilities or productivity;

d) Its use must be minimal and take place substantially outside of normal working hour

e) It should comply with the terms of this policy and all other policies which might be relevant (to include but not limited to):

i. Srei's Equal Opportunities Policy

ii. Anti-Harassment Policy

iii. Data Protection Policy

iv. Disciplinary Procedure.

22.2.21 Employees are also personally responsible for what they communicate on social media sites outside the workplace, for example at home, in their own time, using their own equipment. They must always be mindful of their contributions and what they disclose about the company.

22.2.22 General rules for social media use

a) Do not post or forward a link to any abusive, discriminatory, harassing, derogatory, defamatory or inappropriate or malicious link/content. This includes potentially offensive or derogatory remarks about any other individual;

b) Employees should never disclose commercially sensitive, anti-competitive, private or confidential information. If they are unsure whether the information you wish to share falls within one of these categories, then should discuss this with the corporate communication team;

c) Do not post material in breach of copyright or other intellectual property rights.

d) Be honest and open, but be mindful of the impact your contribution might make to people's perceptions of the company.

e) Employees are personally responsible for content they publish – be aware that it will be public for many years.

f) When using social media for personal use, use a disclaimer, for example: 'The views expressed are my own and don't reflect the views of my employer'. Be aware though that even if you make it clear that your views on such topics do not represent those of the organisation, your comments could still damage our reputation.

g) The employee's online profile must not contain the company name.

h) Employees should avoid social media communications that might be misconstrued in a way that could damage our business reputation, even indirectly.

i) Do not post anything that may be found offensive, insulting, obscene and / or discriminatory by colleagues, customers, clients, business partners, suppliers or vendors.

j) Do use privacy settings where appropriate but bear in mind that even comments in a restricted forum may be passed on.

k) If employees have disclosed your affiliation as an employee of Srei, then they must ensure that the profile and any content posted are consistent with the professional image you present to client and colleagues.

l) If employees are concerned or uncertain about the appropriateness of any statement or posting, refrain from posting it until the same is discussed with reporting manager.

m) If it is observed that social media content that disparages or reflects poorly on Srei, the same should be brought in the notice of corporate communication team.

23. Endpoint Security

23.1 All servers, desktops and access points to Organization's network within the Organization or on outsourced vendor's facility must be protected against malicious code with anti-virus software and processes must ensure early detection, efficient containment and eradication of malicious code within the network of the Organization.

23.2 Anti-virus software should be installed on all servers, laptops and PCs with risk of virus infection. All operating systems should have anti-virus installed. ASP should certify that anti-virus is installed in the operating systems provided by them.

23.3 USBs should be disabled on all the PCs and laptops, should be enabled as and when necessary. Enabling request will be recommended by the respective Department Heads and Head – IT Infra, and will be approved by CISO.

23.4 Anti-virus software should be updated and deployed with latest signature patterns at regular intervals at all end points of the Organization.

23.5 Anti-virus agent should automatically scan any externally connected storage media like Pen drive, CD Drive etc., immediately on connection.

23.6 If feasible, the anti-virus agent should be configured to accept updates from a backup anti-virus server, in case the primary server fails.

23.7 Anti-Virus solution should provide Endpoint protection like denial controls and data leakage prevention.

24. Data Protection

All identified data shall be protected in all phases of its life cycle including collection, processing, transmission, storage, exchange and retirement. Privacy of Personally Identified Information of the Organization shall be ensured.

24.1 Data Identification

Business Data	Business data refers to information proprietary to the Organization which includes financials records, sales, marketing, and products data.
Personally Identifiable Information	All data which can uniquely identify an individual, either Organization's customer or employee, is called as Personally Identifiable Information (PII).

24.2 Roles and Responsibilities for Data Protection

CTO and CISO are jointly responsible for Data protection, along with Business department as given below:

Head Of the Department as Information Owner	Head of the Department shall be the Information Owner and shall be responsible for respective Organization's business information asset. Responsibilities would include, but not be limited to: • Nominate Information sub-owners for each Business unit. • Assigning business information classification and periodically reviewing the classification to ensure it still meets business needs.
Business Head as Information Sub-owner	Business Head, shall act as Information Sub-Owner and shall be responsible for following in co-ordination with respective application owner: • Ensuring security controls are in place commensurate with the classification. • Reviewing and ensuring currency of the access rights associated with information assets they own. • Determining security requirements, access criteria and backup requirements for the information assets they own.
User manager	The user manager is the immediate manager or controller of an employee. He/she has the ultimate responsibility for all user IDs and information assets owned by Organization employees. In the case of non-employee individuals such as contractors, consultants, etc., user manager is responsible for the activity and for the Organization assets used by these individuals.

	• Informing application owner of the transfer of any employee if the transfer involves the change of access rights or privileges. • Reporting any security incident or suspected incident to the Information Security function. • Ensuring that employees are aware of relevant security policies, procedures and standards to which they are accountable.
End user	• Maintaining confidentiality of log-in password(s) • Ensuring security of information entrusted to them as a part of job responsibility • Adhering to all information security policies, procedures, standards and guidelines • Promptly reporting security incidents to management
Application Owner	Application Owner, as Information Custodian, is the delegate of the information owner with primary responsibilities for dealing with management of information systems. Responsibilities include, but are not limited to, the following: • Implementation of security controls according to information classification assigned by business owner. • Establishing user access criteria, availability requirements and audit trails for their applications. • Performing or delegating the following: day-to-day security administration, approval of exception access requests.

24.3 Data Inventory Maintenance

An inventory should be maintained of identified data (categories of data) along with following information: Data name, DPO (Data Privacy Officer), Data storage location, Data Classification, Business Justification of Data collection / storage, Data Retention period and Data retirement and disposal dates. The inventory should be reviewed periodically by respective DPO. DPO will report to CTO.

24.4 Data Classification

Based on its risk rating and sensitivity to business operations, all identified data should be classified under one of the following categories:

Classification	Description	Examples
Public	Information that is available to the general public and intended for distribution outside the Organization. This information may be freely	• Information available on organization's website • Organization's circulars / guidelines for customers

Classification	Description	Examples
	disseminated without potential harm.	• Organization's new scheme brochures
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.	• Organization's policies and procedures • Minutes of Meeting (internal within interested departments)
Confidential	Information that is proprietary to the Organization and its unauthorized disclosure could adversely impact the Organization, its employees and its customers.	• Customer's and employee's PII • Customer's account information • Organization's future investment plans
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.	• Information on Organization's performance (profits, NPAs, any other information that can affect Organization's stock prices), before it is published • Occurrence of fraud against the Organization • Operational shortcomings that can affect the Organization's reputation

Head of the respective business unit is responsible for Data Classification.

24.5 Data Storage

24.5.1 Data Storage and Retention should be done with measures adequate to its classification. Confidential data should only be stored in locations which are approved by DPO. OS default encryption feature should be used for securing official data stored on users' desktops. Data backup on media should be protected with encryption and/or password as per data classification.

24.5.2 Data security is a set of standards and technologies that protect data from intentional or accidental destruction, modification or disclosure.

24.5.3 The primary aim of data security is to protect the data that an organization collects, stores, creates, receives or transmits. Compliance is also a major consideration.

24.5.4 DLP is a strategy/ tool for making sure that end users do not send sensitive or critical information outside the corporate network.

24.5.5 With DLP, administrators can use several methods to classify data:

24.5.6 Use predefined scripts, dictionaries, file-types, and regular expression (regex) patterns to start classifying data right away.

24.5.7 DLP policies enable monitoring and control of the flow of sensitive data throughout an organization. Depending on your DLP configuration, you can set up policies to monitor information sent via email and over HTTP and HTTPS channels, Endpoint channel and ensure all communications are in line with applicable regulations and compliance laws.

25. Operating System Security

The most secure implementation of the operating system should be selected at installation time and user access to operating system should be restricted and monitored. All operating systems supplied by external application service providers should be tested for this compliance. All operating systems, purchased directly by the Organization or supplied by the ASP, should be kept current against security patches released by the vendor.

25.1 Licensing

CTO shall ensure that adequate licenses are maintained for the operating system and any relevant licenses software.

25.2 User authentication

25.2.1 User Access and Password Management policy should be referred for authentication of user, creation of user ID, assignment of privilege levels, password management, user access review, logging and related activities.

25.2.2 Access to operating systems should use secure log-on mechanisms; the system / application must not provide any help to the user during the log-on process that could aid an unauthorized user.

25.2.3 Logging should be enabled to track critical system activities. Logs provide the audit trail and play an important role in tracking malicious users in the event of a compromise.

25.3 Patch updating

25.3.1 The IT department is responsible for ensuring that all necessary security patches and hot fixes for the operating system are applied. Respective application owner is responsible for devising formal procedures for tracking and analysis the current security patches and hot fixes and applying the applicable security patches to Operating systems.

25.3.2 **Several non-essential services** are enabled during a default installation of OS. All the non-essential services should be disabled. For example, Simple Network Management Protocol (SNMP) is a protocol that gets enabled as part of default system installation. Malicious user can use the default SNMP passwords and read / modify system settings. If SNMP service is not required by the Organization, the service should be disabled.

26. VPN usage and access policy

26.1 Intent

The purpose of this document is to provide guidance on secure access for all users to Srei's network over the Internet via Virtual Private Network (VPN) service.

26.2 Objective

The objectives of VPN Access and Usage Policy are:

26.2.1 Protect the security and functionality of Srei's IT Resources and the data stored on those resources

26.2.2 Safeguard the privacy, property rights and data of the organization

26.2.3 Preserve the integrity and reputation of Srei

26.2.4 Comply with applicable business, legal and regulatory requirements

26.2.5 Comply with Srei's applicable policies, standards, guidelines, and procedures

26.3 Scope

This policy applies to the access and usage of VPN services of Srei Equipment Finance Limited (SEFL) and its Affiliates, Subsidiaries and Joint Ventures (hereinafter referred to as Srei), which can be hosted in Srei's own data centre or that of managed service provider.

26.4 Applicability

This policy applies to all users who will utilize VPN to access Srei's network – they can be employees, trainees (Including Management Trainees), suppliers, consultants, temporary employees and personnel affiliated with third parties. This policy applies to access and usage of VPN services that are directed through IPsec and SSL through VPN devices and authentication.

26.5 VPN Usage and access Policy Guideline

26.5.1 VPN Terms of Use

a) It is the responsibility of all users with VPN privileges to ensure that unauthorized users are not allowed access to Srei's network and associated resources. At no time should any user share their username or password with anyone, not even family members.

b) All network activity during a VPN session is subject to Srei's Information Security Policy. All individuals and machines, while using Srei's VPN service, including company-owned and personal device, are a de facto extension of Srei's network and as such should adhere to Srei's applicable policies.

c) All existing policies related to data standards, data privacy, and confidentiality are applicable and should be followed when connecting to Srei's systems remotely via VPN.

d) All devices connected to Srei's internal network via VPN should use a properly configured, up-to-date operating system and anti-virus software; this includes all personally-owned devices. Antivirus software is available for all employees.

26.5.2. Guidelines for Access

a) Remote access to Srei's network using the Internet is only allowed via a VPN connection, and access to applications further may be obtained via Terminal Server if needed.

b) Any employee who has been allotted a laptop by Srei is eligible for VPN connection.

c) All VPN access is using domain (Srei's Active Directory) account ID of the user as authentication is integrated with Active Directory.

d) Generic / common accounts shall not be granted VPN connection due to lack of accountability. These accounts are typically shared among several users and there is no way to trace a specific user back to the account at any given time. All VPN access is using named account of the user in Active Directory.

e) Temporary employee and trainee (summer trainee/management trainee/intern) accounts shall be granted VPN access by default only if they have been given laptop by Srei. However, as per policy, their access shall happen using their domain account ID.

f) Supplier, consultant accounts may be granted VPN access on a case to case basis. Supplier accounts are setup specifically for outsourced resources to access Srei network for support purposes. Supplier accounts should be mapped to a Srei employee who will be responsible. That Srei employee bears responsibility for the account and its use by the outsourced resource. If the supplier account does not already exist in Srei's Active Directory, a request to establish one should be made at the same time VPN access is requested. Once VPN access for supplier/consultant is authorised by HOD, the Information & Cyber Security Team shall assess the risks of granting him VPN connection and suggest on counter measures. No local account made in firewall/VPN device shall be used.

g) In order to use the VPN, user needs a connection to the Internet from his/her location of presence for which Srei is not responsible.

h) Authentication to VPN is governed by the company – in addition to password, a second level of authentication in the form of a onetime password transmitted via mobile SMS facility is required.

i) After successful authentication, what all Srei resources user is authorised to use, will depend on his/her job profile.

j) VPN users will be automatically disconnected from the Srei's network after a period of inactivity. Save your work often.

k) Only resources hosted by Srei are secured by the VPN. Other resources accessed during a VPN session (e.g. external internet websites) are not secured by the Srei VPN.

l) Exceptions to this policy will be handled on a case to case basis by CTO.

26.6 Policy Compliance

26.6.1 Compliance Measurement

The Information & Cyber Security Team will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, monitoring, business tool reports, internal and external audits, and feedback to the policy owner. Status of the compliance will be reported to CTO and CRO on a continuous basis.

26.6.2 Exceptions

Any exception to the policy would be discussed with IT Ops, approved by the Information & Cyber Security Team and CTO before being enforced.

26.6.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

27. Risk Management

27.1 Policy Statement

The Organization shall identify, analyse and mitigate risks which affect confidentiality, integrity and availability of information system assets. The Organization will be entering into tie-ups with various application service providers (ASP) / vendors for implementing modern IT initiatives for resolving issues which may lead to compromising confidentiality and integrity.

27.2 Standards and Procedures

27.2.1 Risk Assessment Methodology

A risk assessment methodology should be identified that is suitable to the organization and the identified information security, legal, statutory and regulatory requirements. The risk assessment methodology should ensure that risk assessment produces comparable and consistent results.

27.2.2 Asset Identification and Classification (Asset management)

a) All assets should be identified by respective departmental heads and an asset inventory should be maintained. The asset may be of the following types:

- **i.** Information Assets that include data files, e-records, system documentation, user manuals, training material, operational procedures for IT management, software licenses, source codes, business continuity plans, contracts, guidelines, HR records etc. as kept in electronic formats. Document in paper would also constitute Information Assets. Some of the examples include contracts, company documentation, business results, purchase document, invoices, license agreement, escrow agreements etc.
- **ii.** Software Assets that include business applications, operating systems, databases, knowledge management application, development tools, utilities etc.
- **iii.** Physical assets that include servers, networking equipment, security devices, backup media, printers, biometric devices, server racks, desktops, laptops etc.
- **iv.** Services and processes that include computing, telecommunications, power, general utilities like air conditioning, alarm systems, fire prevention, hardware and application support etc.
- **v.** People assets that include organization's employees.

b) All information system assets should have a designated owner. Asset owner's primary responsibility is to maintain the confidentiality, integrity and availability of the asset. Asset owner shall define the access rights for the assets.

c) All assets including hardware, software, physical assets, and media should be reviewed for risk assessment by respective designated owner at least once in a year. It should also be ensured that all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, which are not required to carry out job responsibilities, are removed/ disabled from hardware before providing to end-users.

d) All information system assets of the Organization should be classified by the asset owner in consultation with the Information & Cyber Security Team based on their business value and impact to business operations.

e) Asset value should be based on level of three parameters i.e. Confidentiality, Integrity and Availability of that asset to Organization's business as High, Medium and Low. The highest value among three parameters should be assigned as Asset value. E.g. Confidentiality=High, Integrity=Medium and Availability=Medium, then asset value will be High, based on confidentiality level which is highest among three parameters.

f) The level of Confidentiality, Integrity and Availability should be valued in terms of business value and impact of Information System assets for continuance of business operations of the Organization as follows:

Asset Value	Highest of C, I, A	• If either C or I or A for the asset is 3, then the asset is classified as High • If either C or I or A for the asset is 2 then the asset is classified as Medium • If either C or I or A for the asset is 1 then the asset is classified as Low

Score	Label	Confidentiality Meaning
1	Low	Public to everyone
2	Medium	Public to SREI, but not outsiders, Moderately confidential
3	High	To named individuals / group members only, Highly confidential

Score	Label	Integrity Meaning
1	Low	The unauthorized modification or destruction of the information could be expected to have limited effect on the organizational operations or assets.
2	Medium	The unauthorized modification or destruction of the information could be expected to have serious effect on the organizational operations or assets
3	High	The unauthorized modification or destruction of the information could be expected to have catastrophic adverse effect on the organizational

Score	Label	Availability Meaning
1	Normal	The disruption of access to or use of the asset could be expected to have limited adverse effect on the organizational operations or assets.
2	Essential	The disruption of access to or use of the asset could be expected to have serious adverse effect on the organizational operations or assets.
3	Critical	The disruption of access to or use of the asset could be expected to have catastrophic adverse effect on the organizational operations or assets.

g) Information may also be classified based on its sensitivity to business operations. Asset owner should classify the information in consultation with the Information & Cyber Security Team based on a defined criteria issued by the Information & Cyber Security Team. The Organization classifies information as one of the following:

Classification	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.

h) Asset owner may periodically review the classification given to the information or valuation of an asset based on changes in business environment.

i) Information Handling Mechanism

Sl. No.	Controls	"Public" and "Internal"	"Confidential" and "Top Secret"
1	Labelling	No specific requirement to label information at this classification level, unless likely to be accessed by third parties.	Documents should include the label "Confidential" or "Top Secret", as appropriate, in the header or footer of each page.
2	Hard Copy Storage	No restrictions for printed storage.	Store within a secure closed container, which can include a locked cabinet or locked office.
3	Email Restrictions	No restrictions for information included as email attachments.	Password-protect documents or data before attaching to any email message.
4	Internal Access (within SREI)	No access restrictions within the organization.	Obtain Information Owner's approval prior to granting access to information.
5	External Access (Third Parties)	No restrictions on legitimate need for access by external parties, although consideration should be given to labelling documents "Internal Use Only" when appropriate.	External parties to sign formal confidentiality agreements prior to information access.

27.2.3 Risk Assessment

a) Risk Assessment should be performed by designated owners, in consultation with the Information & Cyber Security Team, by following three steps as briefed below:

i. Risk identification is to find, recognize, and describe the risks that could affect the achievement of objectives which should be met through an application.

ii. Risk analysis is to understand the nature, sources, and causes of the risks that are identified and to estimate the level of risk. Risk analysis exercise should also study impacts and consequences and examine the controls that currently exist. Risk analysis is elaborated in subsequent clauses.

iii. Risk evaluation compares the estimated risks, established by means of a risk analysis, with a set of risk criteria. This is done in order to determine how significant the risk really is i.e. whether level of risk is acceptable or not.

Guidelines on how to conduct Risk Assessment at branches / offices shall be issued by the Information & Cyber Security Team.

b) The asset owners should identify various risks based on the identified threats and vulnerabilities and the impacts that losses of confidentiality, integrity and availability may have on the assets. Given below is a brief description on threat and vulnerability.

i. A threat is a potential cause of an incident that may result in harm to system or organization. Threats can originate from accidental or deliberate sources or events. Example: Unauthorized access to information, systems or software.

ii. Vulnerability is a weakness of an asset or group of assets than can be exploited by one or more threats. The weakness could be exploited by threats causing unwanted incidents that might result in loss, damage or harm to these assets and the business of the organization. Example: No or weak password and account policy on systems, applications or database.

c) Likelihood is categorized as “Very High”, “High”, “Sometimes”, “Seldom” or “Very rarely” based on the likelihood of occurrence. The following table defines the likelihood ratings:

Likelihood Rating	
Very rarely (1)	The threat has very rare probability of occurrence
Seldom (2)	Probability of the threat compromising the vulnerability is seldom.
Sometimes (3)	Threat can occur sometimes.
High (4)	The threat has high probability of occurrence
Very High(5)	The threat has very high probability of occurrence.

d) Vulnerabilities are rated as “Critical”, “Very High”, “High”, “Medium” or “Least” based on ease of exploit and level of protection currently present on the asset. The following table defines the vulnerability ratings:

Vulnerability Rating	
Least (1)	Little or no effect if the asset vulnerability is compromised.
Medium (2)	Some effect if the asset vulnerability is compromised.
High (3)	Considerable effect if the asset vulnerability is compromised.
Very High (4)	Great effect if the asset vulnerability is compromised.
Critical(5)	Catastrophic effect if the asset vulnerability is compromised

e) Risk assessment procedure of the Organization follows a zero-control approach for the first time for new systems / applications. In this approach, all the threats and vulnerabilities a particular asset may be exposed to are identified and appropriate controls are selected to mitigate the vulnerabilities and reduce the risk to acceptable levels.

f) Afterwards, risk assessment procedure should follow an ongoing approach for existing systems/applications. This approach takes into account all the existing controls and their effectiveness in terms of residual risks and assessment for new vulnerabilities and controls required.

g) The ranking of risks is based on a qualitative and quantitative method. Risk ranking is arrived based on following formula:

Risk Rating = Asset value × Vulnerability Value x Likelihood Value

27.2.4 Risk Acceptance Level

a) Based on the above matrix the risks can be ranked on a scale of 1 to 75. Threshold or acceptable level of risk rating is <=24.

b) The result of the risk assessment will be reported by CISO to the IT Strategy Committee with its recommendation regarding the Risk Acceptance level. Once the same is approved by the Committee all risks above the acceptance level would need a mitigation plan which would be monitored by the CRO. CRO will review and provide approval or advice next steps to minimize/mitigate for any risk which is above the risk acceptance level of the Organization.

c) All risk which is above the acceptable limit and cannot be mitigated will be has to be considered as the residual risk which would need to be approved by the IT Strategy Committee.

27.2.5 Risk Management

Risk Management is the overall responsibility of the asset owner with the assistance of the CISO wherever applicable. The asset owner should implement controls identified in the risk analysis phase in order to mitigate the risk.

The options for Risk Management can include the following:

a) Avoid – In this case the vulnerability, itself is removed or replaced. Avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk.

b) Treat / Reduce – Controls are implemented to reduce the level of risk or removing the source of risk or change the likelihood or change the consequence.

c) Transfer / Share – The liability is transferred to an internal or external entity through an agreement or sharing the risk with other parties (e.g. contracts and risk financing, insurance policy, etc.).

d) Accept – Whenever control cannot be identified or cost of implementation outweighs the potential loss, a decision can be taken to accept the risk. In such scenario, the decisions should be documented and approved by the Risk Management Committee.

27.2.6 Residual Risk

The asset owner should measure the residual risk after implementing the controls. Residual Risk is the risk that remains even after risk treatment. This may be due to cost of implementation is higher than the potential loss. If residual risk level is above Risk Acceptance level after risk treatment, the decision to accept the risk should be taken by application owner with approval of IT Strategy Committee. Whenever control cannot be identified or cost of implementation outweighs the potential loss, a decision can be taken to accept the risk. In such scenario, the decisions should be documented and approved by IT Strategy Committee.

27.2.7 Continuous Monitoring and Review

a) The asset owner should undertake reviews on a yearly basis or based on need, to verify the adequacy of existing controls, residual risk and acceptable level of risks. The asset owner should monitor the implemented controls, measure the control effectiveness.

b) The asset owner should identify any new risks arising due to significant changes made to the assets or business processes. Assets owners should do re-assessment in consultation with the Information & Cyber Security Team in the following scenarios:

i. New assets are introduced into business
ii. New threats and vulnerabilities to assets are identified
iii. Changes in the underlying Technology or IT controls
iv. Change in business objectives or processes
v. External events such as regulatory or legal requirements

28. System acquisition, development and maintenance

28.1 Key Control Objective

Incorporating security controls into applications and systems at the development stage, minimizes the company's risk exposure and reduces costs by removing the need to retrofit security, post-development. It is also important that Srei retains its rights to, and control of, intellectual and proprietary information that is created during the development of systems or applications for the company.

28.2 Controls

28.2.1 The security organization must be advised about all new systems or applications, prior to their development. Once informed, the security organization will work with the information owner to perform a security risk analysis, using a formalized security risk analysis process, of the new system or application to ensure that appropriate security controls are identified and incorporated during the development process.

28.2.2 All applications should be assessed for their business criticality and have their data classified. The company's data classification scheme should be used.

28.2.3 Data input validation checks must be incorporated during development, with supporting procedures for managing validation errors.

28.2.4 Output validation checks must be incorporated, to ensure accuracy of information processed.

28.2.5 Processes and procedures should be developed to govern the rollout, deployment, usage and management of encryption techniques, including the keys. Local policies must be developed, where deemed appropriate.

28.2.6 As far as possible, the use of production data when testing systems or applications must not be allowed. Test data must be created and used instead. In the event that production data must be used, it must be anonymized and production level environment controls must be applied to the test environment. In addition, explicit procedures must be followed for the destruction and retention of any such production data following completion of testing.

28.2.7 Procedures must be developed for the maintenance and control of internally or externally developed program source code and executable libraries. At least one program librarian must be assigned to manage these processes.

28.2.8 Formal change management procedures, that provide a consistent approach to initiate, execute and manage changes to various software applications and systems, must be developed and implemented.

28.2.9 Logging and monitoring must be built into critical multi-user systems and applications. All access control mechanisms must include role-based profiles and must allow for clear segregation of duties. Such segregation must prevent users from accessing options for which they have insufficient authorization.

28.2.10 The use of any software utility, application or diagnostic tools/access mechanisms that can circumvent application controls is not permitted, unless explicitly authorized by Srei company senior management.

28.2.11 When changes are made to operating system software, business critical applications must be tested to ensure there has been no new adverse impact on their operability.

28.2.12 Modifications to software must only be carried out after they have been thoroughly tested and it has been confirmed that they do not compromise any security controls within the software.

28.2.13 In addition, such modifications must be in compliance with the terms and conditions of the software agreement. Controls must be put in place to protect the intellectual property that is represented by Srei proprietary software, from potential information leakage opportunities.

28.2.14 Any outsourced software development must be supervised and monitored through the usage of appropriate governance processes.

28.2.15 Srei must develop and implement appropriate patch management systems encompassing controls relating to monitoring vulnerabilities, vendor patches and fixes, and their implementation. Should a business need arise, to not implement one or more identified patches, then such decisions should be risk-assessed, acknowledged and documented.

28.2.16 Secure coding must be practiced in all applications developed / acquired. New applications should be deployed only after User Acceptance Testing (UAT) and Vulnerability Assessment / Penetration Testing (VAPT) and CISO clearance.

29. Information Security Incident Management

29.1 Key Control Objective

An 'incident' is a malicious event that leads to (or may lead to) a significant disruption of business. It is the act of violating an explicit or implied security policy. Examples: Attacker posts company credentials online, attacker steals customer credit card database, worm spreading through network, unwanted disruption or denial of service, changes to system hardware, firmware or software characteristics and data without the Application Owner's knowledge, etc.
In order to maintain business operations, the effects and impact, of any security breach, to the company must be avoided.

29.2 Controls

29.2.1 The Company to take seriously any threats – real or suspected – to the security and integrity of Company IT assets. Users must immediately report any suspected security problem or misuse of Company IT assets to the appropriate supervisor or by contacting the manager in charge for information security or information technology Helpdesk.

29.2.2 Formal security incident management procedures must be developed and implemented. These procedures must explicitly define roles and responsibilities as well as reporting and escalation procedures. They must ensure that all relevant parties are informed on a timely basis.

29.2.3 Delivery/functional leaders and all members of staff must be made aware of how to identify a security breach and whom to contact in such an event.

29.2.4 Srei should assign responsibility for the quick, effective and orderly response to information security incidents. Such responsibilities should be documented and appropriately assigned.

29.2.5 When a breach of security is suspected or conveyed, consideration must be given to isolating or closing down the affected system(s) from the rest of the network, to limit exposure, in accordance with agreed procedures. Any accounts or systems that are impacted must be investigated.

29.2.6 For a security incident or potential breach, user must cooperate with the investigating team by all means and surrender his/her system immediately if required, in accordance with agreed procedure.

29.2.7 Formal risk mitigation procedures must be developed and approved by appropriate personnel to deal with the occurrence of any security breach that contravenes legal, regulatory or contractual obligations, the engagement of specialist fraud investigators must be considered in the event of a security breach involving financial loss. Evidence must be collected and retained in accordance with local legal requirements.

29.2.8 The Information & Cyber Security Team function must be informed in a timely manner in the event of a security breach that may have an impact on other member firms or on the Srei network as a whole. It is the responsibility of the Information & Cyber Security Team to inform the corresponding member firms in a timely manner about such incidents. Formal agreed authorization procedures must be followed when a subsidiary invokes its business continuity plan in the event of a security breach. Comments on potential or actual security breaches must not be made to individuals or groups, either internally or externally, without the explicit, formal approval of authorized subsidiary management.

29.2.9 In case of intentional violation of Information Security Policy, appropriate disciplinary action as deemed fit may be initiated by HR department, as per the incident severity and impact and recommendation from IT. All corresponding evidence and preventive/corrective measures must be documented and retained for future reference and analysis.

29.2.10 All incidents should be reported to the top management / regulators as per applicable guidelines. CTO and CISO are jointly responsible for such reporting.

29.2.11 SREI shall maintain a consolidated list of incidents, their criticality, root cause analysis and remedial actions with date and timestamps so that there is a knowledge repository in place for reference in case of a reoccurring security incident (Reference: SREI Security Operations Manual V7).

29.2.12 The management of routine IT incidents is done by the SREI IT Helpdesk Team. The same shall be governed by the "Statement of Work for IBM Integrated Managed Services".

29.3 Turn Around Time (TAT) for Incidents

The below table defines the general framework for TAT:

Turn Around Time (TAT)		
Severity Level	**Response Time**	**Recommended Action / Resolution**
Severity 1	Not more than 30 minutes	Not more than 4 hours
Severity 2	Not more than 1 hour	Not more than 8 hours
Severity 3	Not more than 8 hours	Not more than 72 hours

29.4 Escalation Matrix

The below table defines the generic escalation matrix for incidents:

Escalation Matrix		
Level	**Vendor**	**SREI**
Level 1	First Line of Support	IT Team
Level 2	Client Service Delivery Lead	Operations Head
Level 3	Project Director	CTO

The SLA cut-off for escalation to Level 2 shall be left to the discretion of the application / infrastructure owners or stakeholders. However, escalation to Level 3 must be mandatorily done if SLA is breached.

30. Password Policy

30.1 Objective

It is the objective of Srei management to take appropriate level of logical security measures to ensure that the safety and security of Srei information assets are properly protected from criminal and environmental threats. Hence, Srei has deployed appropriate logical security controls to protect against the risk of theft or unauthorized access to Srei information. The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and maintain a systematic/frequency of change of password.

30.2 Scope

The policies listed in this document apply to all staff who have their user account created in Srei resources, systems like servers, networks, desktops, applications, mobile devices, etc. The user accounts may be normal user account allocated to Srei regular employee, consultant/advisor, trainee, part time faculty, contractor/vendor, intern; or privileged user account like system administrator and application user accounts like user account for applications used by Srei system administrators, network administrators etc.

30.3 Risks Assessment

A non-secure password management may result Srei information asset subject to the following risks:

30.3.1 Risk of unauthorized access to information assets

30.3.2 Risk of theft of information assets

30.3.3 Risk of unauthorized access to systems and network

30.4 Roles and Responsibilities

Roles	Responsibilities
Information Technology	1. Enforcing Password Policy for domain user accounts, privileged user accounts, email user accounts and other application user account 2. Maintaining and monitoring logs for unauthorized access attempt 3. Educating users about password policy
Users	1. Keeping a good knowledge of the Password Policy 2. Memorizing user passwords. Not writing the password anywhere 3. Not sharing the password 4. Avoiding usage of easily guessable passwords

30.5 Policy for Domain, Email and other Application (regular) User Accounts

Accounts allocated to domain, email and application users must abide by the following:

30.5.1 Password will be mandatory for all user accounts.

30.5.2 The minimum length of password for user accounts will be set to at least 8 characters.

30.5.3 The password must include at least one special character and one numeric character.

30.5.4 A password expiration period of 60 days will be set so that users are forced to change their passwords on a regular basis.

30.5.5 Users must change their password immediately after first logon.

30.5.6 The practice of "recycling" or reusing the same password, when prompted for change, will be prevented. A history of 3 passwords will be retained for this purpose.

30.5.7 User IDs / accounts will be disabled after 5 consecutive attempts with incorrect password.

30.5.8 The system will force the user to change the password (assigned by the administrator or Help Desk) at time of initial logon, wherever possible.

30.5.9 The initial password created by administrators or Help Desk will confirm to the password construction standards.

30.5.10 System files holding the authentication data or passwords will be protected from unauthorized access.

30.5.11 Passwords must not be communicated through email or any form of electronic communication and/or written in notebook, paper etc. They can be communicated over telephone and/or individual SMS text only.

30.6 All (System) Privileged User Accounts

All Privileged user accounts (e.g. super user, Administrator in domain/email system/other applications) must abide by the following:

30.6.1 Password will be mandatory for all privileged user accounts.

30.6.2 The minimum length of password for privileged user accounts will be set to at least 8 characters.

30.6.3 The password must include at least one special character and one numeric character.

30.6.4 A password expiration period of 60 days will be set so that privileged users are forced to change their passwords on a regular basis.

30.6.5 Users must change their password immediately after first logon.

30.6.6 In the event, a staff member who has privileged access separates from the organization, IT Helpdesk will ensure that the passwords are changed immediately on his/her last working day. Users will not be allowed to change their passwords within a period of less than 24 hours.

30.6.7 The practice of "recycling" or reusing the same password, when prompted for change, will be prevented. A history of 3 passwords will be retained for this purpose.

30.6.8 User IDs / accounts will be disabled after 5 consecutive attempts with incorrect passwords.

30.6.9 System files holding the authentication data or passwords will be protected from unauthorized access.

30.6.10 Passwords must not be communicated through email or any form of electronic communication and/or written in notebook, paper etc. They can be communicated over telephone or individual SMS text only.

30.6.11 All privileged/Administrator level passwords shall be stored in fireproof safe cabinet. Default Administrator accounts should be renamed, wherever possible.

30.6.12 If any user account is created which is equivalent to Administrator account, the password should be different from that of the Administrator user account.

30.7 Guidelines for Strong Password

30.7.1 Password should contain both upper and lower case characters.

30.7.2 Ensure that passwords have numeric numbers (digit), special characters e.g. ! @ # $ % ^ &.

30.7.3 Passwords must be equal to or more that 8 alphanumeric characters and/or is a passphrase.

30.7.4 Passwords should NOT be individual name, common names, birth days, organization names, family member names, popular places names, dictionary words, or words in a slang, dialect, jargon, etc.

30.7.5 Passwords should NOT have repeated letters, patterns etc.

30.7.6 Try to create passwords that can be easily remembered, yet strong enough. One way to do this is creating a password based on a song title, affirmation, or other phrase. For example, the phrase might be: This May Be One Way to Remember and the password could be: TmB1w2R! or Tmb1W>r~ or some other variation.

30.8 Password Protection

30.8.1 Users shall not share their password with others or shall not reveal the same to others under any circumstances. If they do so then they shall be accountable for the actions taken by the other party with the password.

30.8.2 Do NOT reveal your organization passwords to your friends, relatives, colleagues.

30.8.3 Do NOT reveal your password over email, chat etc.

30.8.4 Do NOT disclose your password in meetings, open forums, etc.

30.8.5 Passwords should never be written down or stored on line.

30.8.6 Do NOT enable “remember password” option in any application or system.

30.8.7 If an account or password compromise is suspected, report the incident to Helpdesk and change the password immediately

31. Software Usage & Licensing Policy

31.1 Objective

The purpose of this Software Usage Policy is to outline the acceptable use of software in SREI and its group companies. Inappropriate use of unauthorized software might expose SREI systems to risks such as virus attacks, compromise of network, systems and services and legal issues. These rules are established to protect the individual employee and SREI against such risks.

31.2 Scope

The policy applies to:

31.2.1 All regular employee (both probationer and confirmed), consultant/advisor;

31.2.2 All trainee, part time faculty, intern;

31.2.3 All third party contractor (including sub-contractor), suppliers, business partners, vendors and service providers

It is mandatory for to comply with this policy while serving SREI's business from any location inside or outside SREI.

31.3 Responsibility

IT Team and all users of IT systems at SREI is responsible to ensure implementation of this policy.

31.4 Categorization of Software

31.4.1 Authorized Software

Business related software (in production environment) can be generically classified as one of

- Licensed
- Freeware

Licensed software is protected by copyright law and has to be purchased with a fee and is generally purchased for a fixed number of users or systems. Licenses can remain valid for ever (perpetual license), or renewed every year/x years (subscription based license) at a cost; licensing is mostly based on number of units/nodes, concurrent users or processors/cores.

Freeware, as the name suggests, is not priced and is available on Internet or other sources for free, but first needs to be authorized for use in SREI before it can be used by certain named users or systems. Freeware can become licensed software in due course of time, depending on manufacturer.

After licensed software is purchased through the proper channels, or freeware has been authorized by the Information & Cyber Security Team and CTO, then only can it be described as authorized software in the organization.

31.4.2 Unauthorized Software

Any software which has not been explicitly approved for use in SREI, including licensed and freeware can be described as unauthorized.

31.5 Policy

31.5.1 Formal change management procedures, that provide a consistent approach to initiate, execute and manage changes to various software applications and systems, must be used.

31.5.2 The use of any software utility, application or diagnostic tools/access mechanisms that can circumvent application controls is not permitted, unless explicitly authorized by the CTO.

31.5.3 Evaluation/trial software is not allowed in the organization, unless for development / testing / demonstration / Proof of Concept purposes or under special, contingency situations approved by the CTO / Head - IT Operations.

31.5.4 Modifications to software must only be carried out after they have been thoroughly tested by the IT Team and approved by the Information & Cyber Security Team and it has been confirmed that they do not compromise any security controls within the software.

31.5.5 In addition, such modifications must be in compliance with the terms and conditions of the software agreement. Controls must be put in place to protect the intellectual property that is represented by SREI proprietary software, from potential information leakage opportunities, if applicable.

31.5.6 Any outsourced software development must be supervised and monitored through the usage of appropriate governance process as deemed fit by IT Operations.

31.6 Guidelines

The following guideline is to advise SREI employees on the correct use of computer software:

31.6.1 All employees can use only that software which is categorized as authorized to be used in SREI.

31.6.2 A standard endpoint (desktop/laptop) issued by IT to a SREI staff comes with standard authorized software, pre-installed.

31.6.3 The sole authority for obtaining/removing any authorized software in SREI lies with CTO only, post which list will be updated and made available again.

31.6.4 After an individual in SREI identifies the need for particular software that is not installed on his/her endpoint and is not listed in the authorized software list either, he/she then can send the requirement to IT Helpdesk who will raise a ticket if needed.

31.6.5 If the software is a licensed one and license available for distribution, Helpdesk will install the same with approval of CISO and / or CTO.

31.6.6 If the software is a licensed one and license not available, cost approval from HOD / Business Head and CFO / Purchase Committee is required for procurement. The HOD / Business Head is expected to write to the Head – IT Operations and CTO, explaining why such software is required by his/her team member(s) giving budget details and if not budgeted, unbudgeted procurement approval from concerned CFO. Purchase Committee takes decision as per Delegation of Authority.

31.6.7 If the software is an authorized freeware but not standard, Helpdesk will keep CISO and CTO informed and install the same.

31.6.8 If the software is an unauthorized freeware, Helpdesk will send to the Information & Cyber Security Team for evaluation and post CTO's approval, it will be installed by Helpdesk.

31.6.9 Wherever applicable, list of authorized software will be updated and adequately informed to IT Operations.

31.6.10 IT Helpdesk will obtain the software from authorized sources and distribute to the user(s), provided it: (1) is appropriately identified and approved for business use; (2) has been approved by the Information & Cyber Security Team in accordance with the organizational, and appropriate departmental security policies; (3) all purchase and/or licensing conditions have been met; (4) software has been scanned for viruses using the most current version of standard anti-virus software; (5) if evaluation software is needed to be installed, IT

Helpdesk will obtain it and install it with written approval of CTO / Head - IT Operations, for a fixed duration only and ensure removal post expiry of evaluation period.

31.6.11 Users directly should not obtain, install and/or store any software (whether freeware or licensed) without the knowledge of IT even if they have the opportunity and the rights. Do not download software installers - executable files (e.g. shell scripts) may be 'Trojan Horses' containing commands designed to corrupt the system or to weaken security. Usage of SREI's Internet facility to download unauthorized software which may deliberately propagate any virus, worm or any other code with malicious intent such as spy-ware, hacking tools, and Trojans is strictly prohibited. If any unauthorized software is found in the end user's endpoint, he/she will responsible.

31.6.12 Once installed by IT, users should comply with all laws and regulations governing data transmission and copyright. Do not duplicate copyrighted or licensed software unless it is explicitly stated that it is allowed.

31.6.13 Updates, service packs and patches to the software shall be installed only by IT, either manually or automatically. Employees should not manually download such updates which may put their systems and client data at risk. For any such requirement, users should inform IT Helpdesk who will do the needful as per the SREI IT Policy.

31.6.14 It is the responsibility of the employees to ensure that they have the latest anti-virus (.DAT) files installed on their computer. If they suspect infection by a virus, they must immediately stop using their computer, disconnect from all networks and notify the IT Helpdesk.

31.6.15 In case you have administrator rights over your desktop/laptop, please ensure that you do not disable the preconfigured settings such as password-protected screensavers, anti-virus agent, other software agents, etc. The absence of any such software should be reported immediately to IT.

31.7 Monitoring

To ensure adherence to this policy, IT Team reserves the right to monitor the activity and data content of all computer equipment housed in SREI work locations (without infringing their privacy policy) and to monitor all SREI computer systems when used for SREI business. Software audits can take place on a periodic basis. SREI employee must report to IT and their HOD the presence of unauthorized or illegal software on SREI systems.

31.8 Exceptions

Any exception to the above policy has to be justified by a valid business requirement. Exceptions have to be justified and approved by the concerned HOD and CTO. Employees need to maintain appropriate documentation as long as necessary to support any such deviations.

32. Management Review

CISO shall ensure review of the Information and Cyber Security process by CRO and act basis his guidance.

32.1 Agenda for Review Meeting

Following inputs make the agenda for each review meeting:

32.1.1 Interested parties' feedback.

32.1.2 Result of independent review

32.1.3 Techniques, products or procedures, which could be used in the organization to improve the Information Security performance and effectiveness

32.1.4 Status of preventive and corrective actions

32.1.5 Reported Information Security Incidents

32.1.6 Vulnerabilities or threats not adequately addressed in the previous risk assessment

32.1.7 Results from effectiveness measurements

32.1.8 Follow-up actions from previous management reviews

32.1.9 Changes that could affect the IS framework and recommendations for improvement.

32.1.10 Trend related to threats and vulnerabilities.

32.1.11 Review of the IS policy

32.2 Recording minutes

32.2.1 CISO summarizes all the decisions, taken in the meeting with CRO, and prepares minutes of the review meeting. Minutes are authorized by CRO and maintained by CISO.

32.2.2 CISO to present the summary of the review by CRO to the IT Strategy Committee and act on its inputs.

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

Annexures

33. Annexure 1 – Acronyms

BCP	Business Continuity Plan
DR	Disaster Recovery
HOD	Head of Department
HR	Human Resources
IDS	Intrusion Detection System
ILL	Internet Lease Line
IPR	Intellectual Property Rights
IPS	Intrusion Prevention System
IS	Information Security
CISO	Chief Information Security Officer
IT	Information Technology
LAN	Local Area Network
NDA	Non-Disclosure Agreement
PDA	Personal Digital Assistant
RACI	Responsible, Accountable, Consulted, and Informed
SLA	Service Level Agreement
VPN	Virtual Private Network
WAN	Wide Area Network

34. Annexure 2 – Definitions

“Authorized Devices” are electronic devices that are owned by a third party, including Users, and have been authorized by the Company to access Company IT Assets or to access, create, send, receive, transmit, store or process Company Electronic Communications or other Company data, files, or information. Electronic devices include, for example, computers, laptops, tablets, cellular phones, pagers, personal data assistants, smartphones, removable storage media (e.g., discs, jump drives), air cards, or the like. Authorized Devices can include Users’ personal electronic devices, if they have been authorized by the Company.

“Company Devices” are electronic devices that are owned, leased, issued or otherwise contracted for by the Company. Electronic devices include, for example, computers, laptops, tablets, cellular phones, pagers, personal data assistants, smartphones, removable storage media (e.g., discs, jump drives), air cards, and the like.

“Company Electronic Communications” are Electronic Communications that are generated specifically in the furtherance of the Company’s business.

“Company IT Assets” are Company Devices and Company IT Systems collectively.

“Company IT Systems” are any system, network, server, or the like that is owned, leased or otherwise contracted for by the Company and that is used to support or facilitate Company Devices, Electronic Communications, or other data or information storage and processing. Company IT Systems include, for example, the Company’s electronic mail system, the Company’s instant messaging system, the intranet, blogs, wikis, facsimile (fax), file transfers, electronic data interchange, audio and video teleconferencing, voice mail, and telephone systems.

“Electronic Communications” are any communication, whether personal or business, made in electronic form. Electronic communications include, for example, information or data transmitted by electronic mail, instant messaging or electronic chat, voicemail, facsimile, file transfer, electronic data interchange, and audio and video teleconferencing, or through the internet or intranet.

“Sensitive Company Information” means information relating to the Company that is confidential, proprietary or otherwise not generally known. Sensitive Company Information includes, for example, project plans, product designs, technical drawings, work product information, confidential Company financial information, business strategies, customers, potential customers, agents, suppliers, Company pricing, securities and trade secret information, legally-privileged information, personally identifiable information of customers or employees, or other proprietary information

“Users” are all employees of the Company and all other individuals who have access to Company IT Assets.

General Policy: Like all other data, files, or other information, Electronic Communications that are accessed, created, sent, received, transmitted, stored or processed via Company IT Assets are Company property. Company Electronic Communications are Company property whether accessed, created, sent, received, transmitted, stored or processed via Company IT Assets or Authorized Devices.