SINGHI CAPITAL FINANCE PRIVATE LIMITED (SCFPL)
Information Technology Policy

Background

The Information Technology Policy (IT Policy) provides an integrated set of protection measures that must be applied across India to ensure a secured operating environment for the lending business of SINGHI CAPITAL FINANCE PRIVATE LIMITED.

Scope

Scope of this IT Policy is the Information stored, communicated and processed within SCFPL and SCFPL's data across outsourced service provider's locations.

This policy applies to all staffs, contractors, service providers, Interns/Trainees working in SCFPL. Third party service providers providing hosting services or wherein data is held outside SCFPL premises, shall also comply with this policy.

Objectives

1. Responsibility

a. Chairperson and Managing Director

The objective of the IT Policy is to provide SCFPL, an approach to managing information risks and directives for the protection of information assets to all units, and those contracted to provide services

The Board of Directors shall delegate the powers, responsibilities and action plans as outlined in this policy as and when required based on the business requirements and the need to manage the IT and Cyber assets in an effective manner.

The overall power to review the compliance with this policy lies with the Information Security Committee (ISC) which comprises of

- Independent Director & Chief Information Security Officer (CISO)

To avoid conflict of interest, CISO shall not be a member of IT department.

The Executive Director would be designated as the Chief Information Security Officer (CISO) and is responsible for articulating the IT Policy that SCFPL uses to protect the information assets apart from coordinating the information security related issues within the organisation as well as relevant external agencies.

ISC shall give recommendations regarding the Information Security risk and responsible for maintenance / review of the IS Policy and also for formulating/review of all sub policies derived from IS Policy.

To avoid conflict of interest in formulation of policy and implementation / compliance the policy has to remain segregated. Therefore, the Information Security Committee (ISC) will be the owner of the IT Policy and Implementation responsibility shall rest with Admin/IT department of SCFPL

All the staffs and external parties as defined in policy are responsible to ensure the confidentiality, integrity and availability of SCFPL's information assets.

Periodic Policy Review

Framework

1 Information Security

The policy shall be reviewed every year or at the time of any major change in existing IT environment affecting policy and procedures, by ISC and placed to Board for approval.

This policy will remain in force until next review / revision.

The purpose of Information Security is to control access to sensitive information, ensuring use only by legitimate users so that data cannot be accessed without proper authorization. Basic tenets of Information Security to be adhered to at all times:

a. Confidentiality – Ensuring access to sensitive data to authorized users only

b. Integrity – Ensuring accuracy and reliability of information by ensuring that there is no modification without authorization

c. Availability – Ensuring that uninterrupted data is available to users when it is needed

d. Authenticity – it is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine

Cyber Security

Cyber Security is ensuring information and communications systems and the information are protected from and/or defended against damage, unauthorized use or modification, or exploitation. Cyber security includes addressing the following aspects in accordance with RBI's guidelines on IT systems in NBFCs. The cyber security guidelines shall cover security aspects pertaining to network, application, data/information apart from cyber security awareness to the users.

The requirements of cyber security will be adhered to keeping in view the IT system environment of SCFPL and the applicability of various requirements.

SCFPL currently uses and shall continue to use digital signatures to protect the authenticity and integrity of important electronic documents and filing statutory returns

SCFPL shall take effective measures to prevent cyber-attacks and to promptly detect any cyber-intrusions so as to respond / recover / contain the fall out.

Awareness & Training

It should be realized that managing cyber risk requires the commitment of the entire organization to create a cyber-safe environment. This will require a high level of awareness among staff at all levels. Top Management and Board should also have a fair degree of awareness of the fine nuances of the threats and appropriate familiarisation may be organized.

All staffs of SCFPL and, where relevant, contractors and third-party users shall receive appropriate awareness training and regular updates in organisational policies and procedures, as relevant for their job function The awareness programme shall be periodically updated keeping in view changes in information technology system, threats/vulnerabilities and/or the information security framework. There shall be a mechanism to track the effectiveness of training programmes through an assessment / testing process.

Sharing of information on cyber-security incidents with RBI

SCFPL shall report all types of unusual security incidents as specified in point No. 2 of Annex I of RBI Master Direction - Information Technology Framework for the NBFC Sector, which deals with Basic Information including Cyber Security Incidents as specified in CSIR Form of Annex I (both the successful as well as the attempted incidents which did not fructify) to the DNBS Central Office, Mumbai.

- IT Enabled Management Information System
- Business Continuity Planning (BCP) and Disaster Recovery
- IT Risk Assessment

It is important to setup a Management Information System (MIS) which is robust and comprehensive in respect of various business functions and as per the needs of the business.

In this regard, a MIS system shall be put in place to assist the Top Management as well as the business heads in decision making and also to maintain an oversight over operations of various business functions.

Disaster recovery planning is a process that includes performing risk assessment, developing recovery strategies and data backup in case of a disaster. SCFPL shall have a business continuity plan and disaster recovery plan to resume normal business operations as quickly as possible after a disaster.

SCFPL shall undertake a comprehensive risk assessment of their IT systems on a yearly basis or as decided by the ISC, keeping in mind of organizational and compliance requirements.

The assessment shall analyse the threats and vulnerabilities to the information technology assets of the organisation and its existing security controls and processes.

The risk assessment will be brought to the notice of ISC, CISO and the Board of the company and serves as an input for Information Security auditors.

Information Systems (IS) Audit

The objective of the IS Audit is to provide an insight on the effectiveness of controls that are in place to ensure confidentiality, integrity and availability of the organization's IT infrastructure. IS Audit shall identify risks and methods to mitigate risk arising out of IT infrastructure such as server architecture, local area networks, physical and information security, telecommunications, etc.

IS Audit forms an integral part of Internal Audit system of the organisation. The organisation shall have adequately skilled personnel in Audit Committee who can understand the results of the IS Audit.

IS Audit should cover effectiveness of policy and oversight of IT systems, evaluating adequacy of processes and internal controls, recommend corrective action to address deficiencies and follow-up. IS Audit also evaluates the effectiveness of business continuity planning, disaster recovery set up and ensure that BCP is effectively implemented in the organization. During the process of IS Audit, due importance shall be given to compliance of all the applicable legal and statutory requirements.

Personnel

IS Audit may be conducted by an internal team of the organisation. In case of inadequate internal skills, organisation may appoint an outside agency having enough expertise in area of IT/IS audit for the purpose. There shall be a right mix of skills and understanding of legal and regulatory requirements so as to assess the efficacy of the framework.

IS Auditors act independently of organisation's Management both in attitude and appearance. In case of engagement of external professional service providers, independence and accountability issues may be properly addressed.

Periodicity

IS audit may be conducted at least once in a year. IS Audit are undertaken prior to the statutory audit so that IS audit reports are available to the statutory auditors well in time for examination and for incorporating comments, if any, in the audit reports.

Compliance

The organisation's management is responsible for deciding the appropriate action to be taken in response to reported observations and recommendations during IS Audit. Responsibilities for compliance/sustenance of compliance, reporting lines, timelines for submission of compliance, authority for accepting compliance should be clearly delineated in the framework. The framework may provide for an audit-mode access for auditors/ inspecting/ regulatory authoritie

Computer-Assisted Audit Techniques (CAATs):

The organisation shall adopt a proper mix of manual techniques and CAATs for conducting IS Audit. CAATs may be used in critical areas (such as detection of revenue

leakage, treasury functions, assessing impact of control weaknesses, monitoring customer transactions under AML requirements and generally in areas where a large volume of transactions are reported) particularly for critical functions or processes having financial/regulatory/legal implications.

Roles and Responsibilities : Board of Directors

Approving the IT Policy

Information Security Committee (ISC)

- **Members of the Committee –** Chairperson & Managing Director, 1 Independent Director, Chief Information Security Officer, Expert from IT Department.
- **Chief Information Security Officer –** Executive Director
- **Convener –** Company Secretary
- **Periodicity of Convening –** Once in a year.

Responsibility/Role of the Committee:

The roles and responsibilities of the various stakeholders pertaining to the IT Policy are as follows

- Developing and facilitating the implementation of information security policies, and procedures to ensure that all identified risks are managed within a SCFPL's risk appetite.
- Reviewing the position of security incidents and various information security assessments and monitoring activities across the SCFPL
- Reviewing the status of security awareness programs
- Assessing new developments or issues relating to information security
- Reporting to the Board of Directors on information security activities.
- Conducting regular ISC meetings (at least once in 6 months) and maintenance of MOM

Chief Information Security Officer (CISO)

Provide support to the Board and ISC in establishing, implementing, monitoring, reviewing, maintaining and improving the overall Information Security of the organization

- Coordinating the ISC meetings
- Coordinating information Security initiatives in the organisation
- Driving and monitoring the ISC directives in the organisation
- Updating ISC about Information Security initiatives, issues and incidents
- Facilitating and Conducting risk assessments of Information Assets used and recommend mitigation controls
- Promote security awareness amongst staffs, customers and service providers

Heads of Departments / General Managers

- The Heads of departments / General Managers are responsible for managing information risk in their respective business as part of their wider risk management responsibilities
- Providing resources and support to the departmental users for information security implementation within SCFPL
- Ensuring security controls are in place, as recommended by ISC, within their departments / business functions
- Determining access criteria and back-up requirements for the information assets / applications they own.

Technology Infrastructure Service Providers

- Infrastructure services shall be provided by strategic outsourced partners with Service Level agreements. The service providers are custodians of IT assets on behalf of SCFPL and are responsible for the implementation and operation of the infrastructure as appropriate to meet the Confidentiality, Integrity and Availability ratings specified by SCFPL
- Develop Standard Operating Procedures (SOP's), Security Guidelines for the assets managed.
- Manage IT assets as per SCFPL approved policies and procedures.

Application Developers

Application systems (including both business applications and generic supporting software, for example, middle-ware, databases) may be developed and maintained by an internal IT function or by a third party. These parties are responsible for:

- Ensuring that systems are developed and maintained, incorporating user requirements and information security requirements that are in adherence to SCFPL Policies

- In conjunction with the provider of the underlying technology infrastructure, for ensuring that information risk is adequately managed in development and test environments and report to SCFPL IT Security

End Users

- Responsible and accountable for activities associated with an assigned account, as well as assigned equipment and removable media;
- Protect secrecy of passwords and Business Information.
- Report known or suspected security incidents

Audit Team

Policies, Procedures and Guidelines

- Data Classification
- Acceptable IT Usage

Conduct information Security audits to check compliance against Policies and procedures.

To ensure that Confidentiality, integrity and availability of information is maintained, a data classification scheme has been designed. The level of security to be provided to the information will depend directly on the classification of the data. The classification of the data shall be done by Heads of Departments / General Managers for their respective departments / business functions

It is imperative to ensure that all the users and staff at SCFPL are aware of their responsibilities towards the IT Resources of SCFPL. The following guidelines shall be adhered to:

- SCFPL staffs have been provided with a company desktop / laptop or portable electronic device. It is the staffs' responsibility for the proper care and use of their desktop / laptop / Portable Electronic Device, data and accompanying software while using the same
- All electronic communication should be courteous, professional and business like as they may be subject to discovery in both criminal and civil proceedings.
- Forwarding of incorrect information or inadvertent distribution can occur more easily than with other means of communication so care needs to be taken to ensure that particularly sensitive, controversial or confidential information is not sent via the

internet.

- Intellectual property guidelines are to be observed
- Employees must not copy, modify or transmit documents, software, information or other materials protected by copyright, trademark, patent or trade secrecy laws without authorization of the owner of such rights in such materials
- Do not use another individual's e-mail account or login - logins and passwords should not be divulged to anyone.
- Accessing another individual's electronic mail and other electronic media should only be done where Employees have a legitimate business need and with the knowledge and approval of that individual or the responsible partner.

Acceptable use

The following are considered as acceptable use:

- SCFPL's IT and electronic communication tools may be used to communicate internally with other internal people or externally with customers, suppliers and other business contacts which enhance productivity.
- Incidental and limited personal use is permitted as long as it does not breach this policy, unreasonably interfere with the performance of the employee's job, consume significant resources, give rise to more than nominal additional costs or interfere with the activities of other SCFPL people.

Prohibited use

Using SCFPL's IT and communication systems for the following is not acceptable and may invite disciplinary/legal proceedings:

- Creating or forwarding hoax messages or chain mail messages
- Personal financial gain or profit
- Soliciting others for non-business activities or in connection with political campaigns or lobbying
- Gambling
- Accessing or downloading pornographic or other offensive/repulsive material
- Representing an employee's personal opinion as that of the firm

- Transmitting material which violates any law or is damaging to the reputation of any person or legal entity
- The infringement of the intellectual property rights of another person or legal entity, such as copyright
- To reveal or publish any proprietary, classified or confidential information of SCFPL and its associates/partners
- Attempting to penetrate computer network security of any legal entity or other system or unauthorized access or attempted access to another individual's computer, e-mail or voicemail accounts or equipment
- To carry messages or material which are defamatory, obscene, harassing, embarrassing, offensive, sexually explicit, intimidating or which seek to discriminate against or vilify any person or group such as offensive, repulsive and explicit messages, images, cartoons, jokes
  or innuendos

Access Control

Data must have sufficient granularity to allow the appropriate authorised access. There is a delicate balance between protecting the data and permitting access to those who need to use the data for authorised purposes. This balance should be recognised. Key aspects in this regard to be considered are:

- Access rights and privileges to SCFPL's information systems and network must be allocated based on the specific requirement of a user's role / function rather than on their status
- The criteria used for granting access privileges must be based on the principle of "least privilege" whereby authorized users will only be granted access to information system and network domains which are necessary for them to carry out the responsibilities of their role or function.
- Care must be taken to ensure that access privileges granted to users do not unknowingly or unnecessarily undermine essential segregation of duties.
- The creation of user access accounts with special privileges such as administrators must be rigorously controlled and restricted to only those users who are responsible for the management or maintenance of the information system or network
- When available audit logging and reporting must be enabled on all information systems and networks

E-mail Security

SCFPL shall implement effective systems and procedures to ensure that e- mails are used as an efficient mode of business communication and implement control procedures so that the e-mail facility is not misused by the users. It also needs to be ensured that e-mail

service and operations remain secure, efficient while communicating within intranet as well as through the internet. Key guidelines to be adhered to include:

- All access to electronic messages must be limited to properly authorized personnel.
- Usage of E-mail system is limited to business needs or any helpful messages.
- All E-Mails must be in compliance with SCFPL's standards regarding decency and appropriate content.

Password Security

The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords and the frequency of change. The following are the minimum guidelines to be adhered to with respect to password security:

- All passwords should be reasonably complex and difficult for unauthorized people to guess, but easy to remember for user
- Employees are advised to choose passwords that are, preferably, at least eight characters long and contain a combination of upper- and lower-case letters, numbers, and punctuation marks and other special characters. These requirements will be enforced with software wherever possible.
- In addition to meeting those requirements, employees should also use common sense when choosing passwords. They must avoid basic combinations that are easy to crack. For instance, choices like "password," "password1" and "P@$$w0rd" are bad from a security perspective.
- It is recommended that the passwords be changed regularly, preferably once in 90 days
- If the security of a password is in doubt– for example, if it appears that an unauthorized person has logged in to the account — the password must be changed immediately.
- Default passwords — such as those created for new employees when they start or those that protect new systems when they're initially set up — must be changed as quickly as possible.
- Passwords may never be shared or revealed to anyone other than the authorized user

Website & Application Security

It may be required to develop and maintain software, applications and add- on modules from time to time. Proper procedures, access controls and security requirements in line with the standard industry practices shall be adhered to during the entire process. Key guidelines pertaining to website and application security include:

- It is recommended that the website is security audited and an audit clearance certificate is issued by a CERT-IN empanelled vendor before hosting in production

environment. The Security Audit should be done every six months or as and when any changes are done to the source code

- Use site-wide SSL certificate which uses at least 2048-bit SHA 256 encryption or higher
- Ensure that the SSL Certificate is valid and keep track of the certificate expiry date and take necessary action to renew/replace the certificate before expiry
- Disable weak ciphers like DES, 3DES, RC4. Use Strong Ciphers like AES, GCM
- Any “non-https” requests received on the website/applications, should be forcefully redirected to “https”
- Ensure that all Websites and Applications and their respective CMS (Content Management System), 3rd party plugins, codes, etc., are updated to the latest versions
- All passwords, connection strings, tokens, keys, etc., should be encrypted with salted hash
- There should not be any plain passwords stored in config files or source code or in database
- All exceptions should be handled appropriately. Custom error pages should be displayed for any errors/exceptions. At no point of time, a portion of source code should be displayed on the page in case of an error or exception
- Ensure that the Computer/system, from where CMS/site updates are being done is installed with the latest OS + Antivirus Updates and Patches. No unauthorized software/cracks, should be installed on the machine.
- In case of the website/application is integrated with any 3rd party Applications or using any APIs for external communication, then ensure that all such communications are done through encrypted channel.

Network Security

Information Security Incident Management

Appropriate controls should be established to ensure security of data in private and public networks, and the protection of connected services from unauthorised access. SCFPL’s Network infrastructure shall be protected from unauthorised access by deploying required firewalls and other security measures

Incident management is required and needs to be established to ensure a quick, effective, and orderly response to security incidents. Such a policy would vary in scope depending on the sensitivity and size of the information systems being managed.

Key guidelines for incident management include:

- Incidents are detected as soon as possible and properly reported
- Incidents are handled by appropriate authorized personnel with ‘skilled’ backup as required
- Incidents are properly recorded and documented
- All evidence is gathered, recorded, documented and maintained properly with proper backup
- The full extent and implications relating to an incident are understood
- Incidents are dealt with in a timely manner and services restored as soon as possible
- Analyse the incidents to learn from them to ensure similar incidents do not recur.
- Learning from the incidents are recorded

Backup & Recovery

In order to safeguard information and computing resources from various business and environmental threats, all business data and related applications shall be backed up on a scheduled basis and in a standardised manner.

The backup and recovery procedures must be automated wherever possible using the system features and be monitored regularly.

Security Awareness

Hardware Acquisition & Maintenance

Data Security Measures

All staffs of SCFPL and, where relevant, contractors and third-party users shall receive appropriate awareness training and regular updates in organisational policies and procedures, as relevant for their job function

During hardware acquisition, it shall be ensured that hardware is of the required quality and helps in meeting the desired business objectives. Hardware thus procured shall be maintained and supported systematically during its lifetime to the extent possible

Appropriate physical, technical and organisational security procedures that restrict access to and disclosure of personal data within SCFPL shall be implemented.

Wherever possible, to prevent unauthorised physical access, damage and interference to the organisations premises and information, critical or sensitive information processing facilities shall be housed in secure area, protected by secure parameters, with appropriate entry controls.

SCFPL shall deploy firewalls and other security procedures to help protect the accuracy and security of sensitive information and prevent unauthorised access or improper use.

Social Media Usage

- Usage of Social Media within TIDCO's network is restricted, unless approved specifically
- Staffs are personally responsible for the content they publish on-line, whether in a blog, social computing site or any other form of user- generated media.
- Staffs are not authorised to publish or discuss the following on Social Media
- SCFPL's confidential or other proprietary information
- To cite or reference Customers, partners or suppliers without their approval
- To use SCFPL's logos or trademarks unless approved to do so.

Compliance

Compliance with Regulatory requirements

- Compliance to statutory, regulatory and contractual requirements such as Information Technology Framework for the NBFC Sector, 2017, directives and recommendations given by Reserve bank of India shall be ensured
- Compliance with terms/conditions and license requirements for the usage of copyrighted software or any other proprietary information/material shall be maintained
- Cross border movement of data shall be in accordance with legal and regulatory requirements
- Records shall be retained and managed based on legal and regulatory requirements

Compliance with Information Security policy & procedures

- Information processing facilities shall be used as per information security policy and acceptable usage policy
- While SCFPL respects the privacy of its staffs it reserves the right to audit and/or monitor the activities of its staffs and information stored, processed, transmitted or handled on any assets/devices/services used by staff
- Exception to security policy and procedure shall be approved through the exception management process

- Policy exceptions shall be reviewed at least annually and as deemed necessary based on security risks envisaged, emerging threats etc.

- Violations or any attempted violations of security policies and procedures shall result in disciplinary/legal actions

Information Systems Audit

Audits shall be conducted to ensure compliance with the information security policies, procedures and guidelines

The use of information systems audit tools shall be controlled and authorised to prevent any possible misuse of tools.