SISL-IT-POL-Supplier Relationship Management Policy

Version No: V 1.0

INTERNAL DOCUMENT

OCTOBER 2025

Document Control

Document Name	SISL-IT-POL-Supplier Relationship Management Policy
Abstract	This document describes supplier relationship management at Share India Group
Security Classification	Internal
Location	Share India Group– Delhi

Authorization		
Document Owner	Reviewed by	Authorized by
IT Team	Head – IT	Head – IT

Amendment Log				
Version	**Modification Date DD MMM YYYY**	**Section**	**A/M/D**	**Brief description of change**
1.0	30th October 2025	Initial Version	A	Final

Distribution list
Designated Officer (DO)
Information Security Steering Committee (ISSC)
ISMS Core Team
Auditors (Internal & External)
All users at Share India Group

Table of Content

1 Introduction

Supplier Relationship Management (also called Vendor Relationship Management) is a set of principles, processes, and tools that can assist the organizations to maximize relationship value with suppliers, minimize risk and management of overhead through the entire supplier relationship life cycle. Supplier Relationship Management has two aspects

- Clear commitment between the supplier and the buyer, and
- The objective of understanding, agreeing, and whenever possible, codifying the interactions between them.

2 Policy Statement

Access by suppliers to any Share India Securities Limited (SISL) asset shall be strictly limited and controlled. An assessment of third party access risks shall be done and appropriate controls to arrive at an acceptable level of residual risk shall be implemented. Third party contracts shall include specification for responsibilities and consequences of unauthorized access to information systems.

3 Scope

The policy applies to

- All process where SISL suppliers have access to the information
- All departments involved in procurement and supplier interaction

4 Roles and Responsibilities

Sr. No.	Role	Responsibility
1.	Designated Officer (DO)	Ensure that this policy is effectively implemented.
2.	Information Security Manager (ISM)	Enforce the policy.
3.	IT / Admin / Human Resource/ Business Operations	Abide by the policy
4.	Suppliers	Abide by the policy

5 Standards and Guidelines

Information security requirements for mitigating the risks associated with supplier's access to SISL's assets shall be agreed with the supplier and documented. This policy shall identify and mandate information security controls to specifically address suppler access to SISL's information.

These security controls shall address processes and procedures to be implemented as well as those processes and procedures that SISL requires the supplier to implement, including:

- Identify and document the types of suppliers, e.g. IT services, logistics utilities, financial services, IT infrastructure components, allowed to access its information
- A standardized process and lifecycle for managing supplier relationships
- Define the types of information access that different types of suppliers shall be allowed and monitor and control the access
- Minimum information security requirements for each type of information and type of access shall serve as the basis for individual supplier agreements based on the business needs and requirements and its risk profile
- Processes and procedures to monitor adherence to established information security requirements for each type of supplier and their access, including third party review and product validation
- Accuracy and Completeness of controls to ensure the integrity of the information or information processing provided by either party
- Types of obligations applicable to suppliers to protect SISL's information
- Handle incidents and contingencies associated with supplier access including responsibilities of both SISL and suppliers
- Resilience and, if necessary, recovery and contingency arrangements to ensure the availability of the information or information processing provided by either party
- Awareness training for SISL's personnel involved in acquisitions regarding applicable policies, processes and procedures.
- Awareness training for SISL's personnel interacting with supplier personnel regarding appropriate rules of engagement and behavior based on the type of supplier and the level of supplier access to the organization's systems and information.
- Conditions under which information security requirements and controls shall be documented in an agreement signed by both parties
- Manage the necessary transitions of information, information processing facilities and anything else that needs to be moved and ensure that information security is maintained throughout the transition period.

5.1 Addressing security within supplier agreements

All relevant information security requirements shall be established and agreed with each supplier who may access, process, store, communicate, or provide IT infrastructure components for, the SISL's information.

Supplier agreements shall be established and documented to ensure that there is no misunderstanding between SISL and the supplier regarding both parties' obligations to fulfill relevant information security requirements.

The following terms shall be considered for inclusion in the agreements in order to satisfy the identified information security requirements:

- Description of the information to be provided or accessed and methods of providing or accessing the information.
- Classification of information according to SISL's classification scheme and if deemed necessary map between its own classification scheme and the classification scheme of the supplier
- Legal and regulatory requirements, including data protection, intellectual property rights and copyright, and a description of how it shall be ensured
- Obligation of each contractual party to implement an agreed set of controls including access control, performance review, monitoring, reporting and auditing
- Rules of acceptable use of information, including unacceptable use if necessary.
- Either explicit list of supplier personnel authorized to access or receive SISL's information or procedures or conditions for authorization, and removal of the authorization, for access to or receipt of the organization's information by supplier personnel
- Information security policies relevant to the specific contract
- Incident management requirements and procedures (especially notification and collaboration during incident remediation)
- Training and awareness requirements for specific procedures and information security requirements, e.g. for incident response, authorization procedures etc.
- Relevant regulations for sub-contracting, including the controls that need to be implemented
- Relevant agreement partners, including a contact person for information security issues
- Screening requirements, if any, for supplier's personnel including responsibilities for conducting the screening and notification procedures if screening has not been completed or if the results give cause for doubt or concern
- Right to audit the supplier processes and controls related to the agreement
- Defect resolution and conflict resolution processes
- Supplier's obligation to periodically deliver an independent report on the effectiveness of control sand agreement on timely correction of relevant issues raised in the report
- Supplier's obligations to comply with the organization's security requirements.

SISL shall ensure that Contracts and Service Level Agreements are signed with the suppliers.

5.2 Information and communication technology supply chain

Agreements with suppliers shall include requirements to address information security risks associated with information and communications technology services and product supply chain.

The following shall be considered for inclusion in supplier agreements concerning supply chain security:

- Define information security requirements to apply to information and communication technology product or service acquisition in addition to the general information security requirements for supplier relationships
- For information and communication technology services, that requires the supplier to propagate SISL's security requirements throughout the supply chain in case the supplier subcontract for parts of information and communication technology service that it provides to SISL.
- For information and communication technology products, that requires the supplier to propagate appropriate security practices throughout the supply chain if these products include components purchased from other suppliers.
- Implement a monitoring process and acceptable methods to validate that delivered information and communication technology products and services are adhered to stated security requirements.
- Implement a process to identify product or service components that are critical for maintaining functionality and therefore require increased attention and scrutiny when built outside of SISL especially if the top tier supplier outsources aspects of product or service components to other suppliers.
- Obtain assurance that critical components and their origin can be traced throughout the supply chain.
- Obtain assurance that the delivered information and communication technology products function as expected without any unexpected or unwanted features.
- Define rules for information sharing regarding the supply chain and any potential issues and compromises among SISL and its suppliers.
- Implement specific processes to manage information and communication technology component lifecycle and availability and associated security risks. This includes managing the risks of components no longer being available due to suppliers no longer being in business or suppliers no longer providing these components due to technological advancements.

5.3 Monitoring and review of supplier services

Monitor and review of supplier services shall ensure that the information security terms and conditions of the agreements are being adhered to and that information security incidents and problems are managed properly.

This shall involve a service management relationship process between SISL and the supplier to:

- Monitor service performance levels to verify adherence to the agreements.
- Review service reports produced by the supplier and arrange regular progress meetings as required by the agreements.
- Conduct audits of suppliers, in conjunction with review of independent auditor's reports, if available and follow-up on issues identified.
- Provide information about information security incidents and review this information as required by the agreements and any supporting guidelines and procedures.
- Review supplier audit trails and records of information security events, operational problems, failures, tracing of faults and disruptions related to the service delivered.
- Resolve and manage any identified problems.
- Review information security aspects of the supplier's relationships with its own suppliers.
- Ensure that the supplier maintains sufficient service capability together with workable plans designed to ensure that agreed service continuity levels are maintained following major service failures or disasters.

The responsibility for managing supplier relationships shall be assigned to a designated individual or service management team. In addition, the organization shall ensure that suppliers assign responsibilities for reviewing compliance and enforcing the requirements of the agreements. Sufficient technical skills and resources shall be made available to monitor that the requirements of the agreement, in particular the information security requirements, are being met. Appropriate action should be taken when deficiencies in the service delivery are observed.

SISL shall retain sufficient overall control and visibility into all security aspects for sensitive or critical information or information processing facilities accessed, processed or managed by a supplier. SISL shall retain visibility into security activities such as change management, identification of vulnerabilities and information security incident reporting and response through a defined reporting process.

5.4 Managing changes to supplier services

Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking into account

the criticality of business information, systems and processes involved and re-assessment of risks.

The following aspects shall be taken into consideration:

- Changes to supplier agreements
- Changes made by SISL to implement
  - Enhancements to the current services offered
  - Development of any new applications and systems
  - Modifications or updates of SISL's policies and procedures
  - New or changed controls to resolve information security incidents and improve security
- Changes in supplier services to implement
  - Changes and enhancement to networks
  - Use of new technologies
  - Adoption of new products or newer versions/releases
  - New development tools and environments
  - Changes to physical location of service facilities
  - Change of suppliers
  - Sub-contracting to another supplier

5.5 Policy on the use of cloud services

SISL shall define and communicate how it intends to manage information security risks associated with the use of cloud services. It can be an extension or part of the existing approach for how SISL would manage services provided by external parties.

Where use of cloud services involves shared responsibility for information security and collaborative effort between the cloud service provider and SISL acting as the cloud service customer, roles and responsibilities for both the cloud service provider and SISL, acting as the cloud service customer, shall be are defined and implemented appropriately.

SISL shall define:

- All relevant information security requirements associated with the use of the cloud services
- Cloud service provider selection criteria and scope of cloud service usage
- Roles and responsibilities related to the use and management of cloud services, which information security controls are managed by the cloud service provider and which are managed by SISL as the cloud service customer;
- How to obtain and utilize information security capabilities provided by the cloud service provider
- How to obtain assurance on information security controls implemented by cloud service providers

- How to manage controls, interfaces and changes in services when an organization uses multiple cloud services, particularly from different cloud service providers
- Procedures for handling information security incidents that occur in relation to the use of cloud services
- SISL's approach for monitoring, reviewing and evaluating the ongoing use of cloud services to manage information security risks
- How to change or stop the use of cloud services including exit strategies for cloud services.

5.5.1 Cloud service agreement terms and conditions

Cloud service agreements are often pre-defined and not open to negotiation for all cloud service providers, SISL shall review cloud service agreements with the cloud service provider(s).

A cloud service agreement shall address the confidentiality, integrity, availability and information handling requirements of SISL, with appropriate cloud service level objectives and cloud service qualitative objectives.

SISL shall also undertake relevant risk assessments to identify the risks associated with using the cloud service. Any residual risks connected to the use of the cloud service shall be clearly identified and accepted by the appropriate management of SISL.

An agreement between the cloud service provider and SISL, acting as the cloud service customer, shall include the following provisions for the protection of SISL's data and availability of services:

- Providing solutions based on industry accepted standards for architecture and infrastructure
- Managing access controls of the cloud service to meet the requirements of SISL
- Implementing malware monitoring and protection solutions
- Processing and storing SISL's sensitive information in approved locations (e.g. particular country or region) or within or subject to a particular jurisdiction
- Providing dedicated support in the event of an information security incident in the cloud service environment
- Ensuring that SISL's information security requirements are met in the event of cloud services being further sub-contracted to an external supplier (or prohibiting cloud services from being sub-contracted)
- Supporting SISL in gathering digital evidence, taking into consideration laws and regulations for digital evidence across different jurisdictions
- Providing appropriate support and availability of services for an appropriate time frame when the organization wants to exit from the cloud service

- Providing required backup of data and configuration information and securely managing backups as applicable, based on the capabilities of the cloud service provider used by SISL, acting as the cloud service customer
- Providing and returning information such as configuration files, source code and data that are owned by SISL, acting as the cloud service customer, when requested during the service provision or at termination of service.

5.5.2 Notification by the cloud service provider

SISL, acting as the cloud service customer, shall consider whether the agreement shall require cloud service providers to provide advance notification prior to any substantive customer impacting changes being made to the way the service is delivered to SISL, including:

- Changes to the technical infrastructure (e.g. relocation, reconfiguration, or changes in hardware or software) that affect or change the cloud service offering
- Processing or storing information in a new geographical or legal jurisdiction
- Use of peer cloud service providers or other subcontractors (including changing existing or using new parties).

5.5.3 Relationship Management

SISL using cloud services shall maintain close contact with its cloud service providers. These contacts enable mutual exchange of information about information security for the use of the cloud services including a mechanism for both cloud service provider and SISL, acting as the cloud service customer, to monitor each service characteristic and report failures to the commitments contained in the agreements.

5.6 Compliance

SISL complies with relevant anti-corruption legislations like the Prevention of Corruption Act, 1988 (India).
SISL's suppliers shall also be subjected to the anti-bribery and anti-corruption compliance requirements.

6 Reference

Ref: SISL-IT-PRO -Supplier Relationship Management Procedure

7 Policy Review Frequency

The policy shall be reviewed annually or when there is a major change within Share India Securities Limited environment.

8 Policy Exception

In case of any deviation against policy guidelines, Risk Acceptance form should be submitted to Designated Officer for approval.

9 Policy Violation Reporting Matrix

Any violation to the policy should be reported to Reporting Manager/Designated Officer

Level	Designation
Level 1	Employee's Reporting Manager
Level 2	Designated Officer
Level 3	MD & CEO