SISL-IT-POL-Human Resource Security Policy

Version No: V 1.0

INTERNAL DOCUMENT

OCTOBER 2025

Document Control

Document Name	SISL-IT-POL-Human Resource Security Policy
Abstract	This document describes Human Resource Security 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

Share India Securities Limited's (SISL) policies and procedures have been developed to reflect and foster sound business practices and high standards of professional conduct by employees, as well as to comply with all applicable laws, regulations and security certification requirements. In establishing certain guidelines and rules of conduct, the company's sole intention is to protect the rights of all employees, to promote maximum cooperation among employees, and to maintain the company's high standards of professionalism, performance and service. None of the policies or procedures laid down here is a contractual commitment by the company, nor does it change the status as an employee at will (which means that either the employee or the company may terminate the employment relationship at any time with or without cause or notice).

2 Policy Statement

Human resources policies and practices shall reduce the risk of theft, fraud or misuse of information facilities by employees, contractors and third-party users

3 Scope

The organization's human resources policies, taken as a whole, shall extend to all the persons within and external to the organization that do (or may) use information or information processing facilities. This shall include:

- Tailor requirements to be suitable for particular roles within the organization for which persons are considered;
- Ensure that persons fully understand the security responsibilities and liabilities of their role(s);
- Ensure awareness of information security threats and concerns, and the necessary steps to mitigate those threats;
- Equip all persons to support organizational privacy and security policies in the course of their normal work, through appropriate training and awareness programs that reduce human error; and
- Ensure that persons exit the organization, or change employment responsibilities within the organization, in an orderly manner.

4 Roles and Responsibilities

Sr. No.	Role	Responsibility
1.	Designated Officer (DO)	Ensure that this policy is effectively implemented.
2.	Human Resource	Enforce the policy.
3.	Employees	Abide by the policy

5 Standards and Guidelines

5.1 Prior to Employment

5.1.1 Screening

Appropriate background verification checks ("screening") for certain candidates and for employment, contractor status, or third party vendor, shall be carried out by the organization or by another appropriate third parties. This shall include screening that:

- Is commensurate with the organization's business needs, and with relevant legal, regulatory, and certificatory requirements;
- Takes into account the classification(s) / sensitivity(ies) of the information or information processing facilities to be accessed, and the perceived risks;
- Takes into account all privacy, protection of personal data and other relevant employment legislation; and
- Includes, where appropriate,
  - Employment track record verification for the last two employments.
  - Verification of employment history including any instance of misuse of information assets during employment / dismissal.
  - Verification of highest academic qualifications and/or certifications.
  - Applicant's criminal court check and current address verification
- Confidentiality or non-disclosure agreements (see Confidentiality agreements) and/or
- Acceptable use of assets agreements.

HR departments shall determine criteria for screening employees posted to computer related / other critical positions of trust by considering the following:

- Background verification of the employee

- Level of access required for the employee - An individual with access to the entire system or to IT infrastructure poses a greater risk than one who can log in at only one workstation and who does not have access to all data.
- Nature of the user's duties and their data access requirements – Duties like posting financial information may pose greater risks.

All personal data collected during the screening process shall be handled in accordance with the provisions of the Digital Personal Data Protection Act, 2023, ensuring lawful processing, data minimization, purpose limitation, and protection of employee privacy

5.1.2 Terms and conditions of employment

Employees, contractors, and third-party users shall agree to and sign a statement of rights and responsibilities for their affiliation with the organization, including rights and responsibilities with respect to information privacy and security. This statement shall include specifications of:

- The scope of access and other privileges the person shall have, with respect to the organization's information and information processing facilities.
- The person's responsibilities, under legal, regulatory, certificatory requirements and organizational policies specified in that or other signed agreements.
- Responsibilities for classification of information and management of organizational information facilities that the person may use.
- Procedures for handling sensitive information, both internal to the organization and that received from or transferred to outside parties.
- Responsibilities that extend outside the organization's boundaries (e.g., for mobile devices and tele-working).
- A formal acknowledgment that they have read, understood, and agreed to abide by SISL's Information Security Policies

5.2 During Employment

5.2.1 Management responsibilities

Management shall require employees, contractors and third-party users to apply security controls in accordance with established policies and procedures of the organization. This shall include:

- Appropriately inform all employees, contractors and third-party users of their information security roles and responsibilities, prior to granting access to sensitive information or information systems (see Terms and conditions of employment).
    - Requirements to act in accordance with the organization's policies, including execution of all processes or activities particular to the individual's role(s);
    - Requirements to protect all information assets from unauthorized access, use, modification, disclosure, destruction or interference.

    - Requirements to report security events, potential events, or other risks to the organization and its assets; and
    - Assignment of responsibility to individuals for actions taken or, where appropriate, responsibility for actions not taken, along with appropriate sanctions.

- Provide all employees, contractors and third parties with guidelines/rules that state the security expectations of their roles within the organization.
- Achieve an appropriate level of awareness of security controls among all employees, contractors and third parties, relevant to their roles and responsibilities.
- Achieve an appropriate level of skills and qualifications, sufficient to execute those security controls.
- Assure conformity to the terms and conditions of employment related to security.
- Motivate adherence to the security policies of the organization, such as with an appropriate sanctions policy.
- Mitigate the risk of failure to adhere to policies, by ensuring that all persons have appropriately-limited access to the organization's information and information facilities.

5.2.2 Information security awareness, education and training

All employees of the organization, and, where relevant, contractors and third-party users shall receive appropriate awareness training in and regular updates of organizational policies and procedures relevant to their job functions. This shall include:

- A formal induction process that includes information security training, prior to being granted access to information or information systems; and
- Ongoing training in security control requirements, legal, regulatory, certificatory responsibilities, and generally accepted security procedures, suitable to the person's rules and responsibilities.

5.2.3 Disciplinary process

There shall be a formal disciplinary process for employees who have committed a security breach. This shall include requirements for:

- Appropriate evidence to initiate investigations (e.g., “reasonable suspicion” that a breach has occurred).
- Appropriate investigatory processes, including specification of roles and responsibilities, standards for collection of evidence and chain of custody of evidence.
- Disciplinary proceedings that observe reasonable requirements for due process and quality of evidence.
- Reasonable evidentiary and burden-of-proof standards to determine fault, ensure correct and fair treatment for persons suspected of a breach.
- Sanctions that appropriately take into consideration factors such as the nature and gravity of the breach, its impact on operations, whether it is a first or repeat offense, whether or

not the violator was appropriately trained, whether or not the violator exercised due care or exhibited negligence.

5.3 Termination or Change of Employment

5.3.1 Termination responsibilities

Responsibilities and practices for performing employment termination or change of employment shall be clearly defined and assigned. This shall include:

- Termination processes that ensure removal of access to all information resources;
- Changes of responsibilities and duties within the organization processed as a termination (of the old position) and re-hire (to the new position), using standard controls for those processes unless otherwise indicated;
- Processes ensuring that other employees, contractors and third parties are appropriately informed of a person's changed status; and any post-employment responsibilities as specified in the terms and conditions of employment, or a contractor's or third party's contract.

All employees, contractors and third parties shall return all of the organization's information and physical assets in their possession upon termination of the employment relationship or contract. This shall include:

- A formal process for return (e.g., checklists against inventory) of the organization's hardware, software and data media.
- A formal process for return or destruction of organizational data of any kind; and
- Where the employee, contractor or third party uses personal equipment, requirements for secure erasure of software and data belonging to the organization.

Access rights to information and information processing facilities shall be removed upon termination of the employment or contractual relationship. This shall include:

- Changes of employment or contractual status include removal of all rights associated with prior roles and duties, and creation of rights appropriate to the new roles and duties.
- Removal or reduction of access rights in a timely fashion; and
- Removal or reduction of access rights prior to the termination, where risks indicate this step to be appropriate (e.g., where termination is initiated by the organization, or the access rights involve highly sensitive information or facilities).

6 Policy Review Frequency

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

7 Policy Exception

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

8 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