Share India
You generate, we multiply

SISL-IT-POL-Information Security Policy

Version No: V 1.0

INTERNAL DOCUMENT

OCTOBER 2025

Document Control

Document Name	SISL-IT-POL-Information Security Policy
Abstract	This document describes information 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

SISL is a mid-sized Regulated Entity (RE) in stock broking sector operating in a highly digitized and technology-driven environment. Given the nature of its business, SISL handles sensitive financial, personal, and strategic data, making it a prime target for cybersecurity threats, data breaches, and regulatory scrutiny. As digital transformation and cloud adoption accelerate, the need for a strong information security posture becomes critical.

2 Policy Statement

This Information Security Policy establishes SISL's commitment to safeguarding its information assets from unauthorized access, disclosure, alteration, or destruction. The policy aligns with SEBI's Cybersecurity and Cyber Resilience Framework (CSCRF), ISO/IEC 27001, and the DPDP Act to ensure the confidentiality, integrity, and availability (CIA) of SISL's information systems.

3 Scope

This policy applies to:

- All SISL employees, contractors, consultants, third-party users, and interns.
- All information assets including servers, databases, applications, cloud services, endpoints, mobile devices, and network infrastructure.

4 Roles and Responsibilities

Sr. No.	Role	Responsibility
1.	ISSC	Provide strategic direction and approve security policies
2.	DO	Lead implementation, monitoring, and reporting of controls.
3.	ISM	Operationalize controls; conduct training and awareness
4.	IT Team	Maintain secure systems and implement technical safeguards
5.	SOC Team	Monitor systems and respond to threats and anomalies.
6.	Users	Comply with policies, report incidents and suspicious activity

5 Information Security Objectives

- To protect SISL's information and IT systems from internal and external threats through preventive, detective, and corrective security measures.
- To ensure compliance with applicable legal, regulatory, and contractual obligations such as SEBI CSCRF, ISO/IEC 27001, and the DPDP Act.
- To establish and maintain a strong culture of information security awareness, accountability, and ownership across all organizational levels.
- To integrate information security into the organization’s strategic planning, operations, and technology adoption to support secure innovation and resilience.
- To ensure the continuity of business operations by implementing appropriate risk management, incident response, and disaster recovery mechanisms.
- To promote continuous improvement through regular audits, vulnerability assessments, and the application of security best practices.

6 Information Security Principles

The following principles govern SISL's approach to securing its information assets and infrastructure. Each principle is implemented and supported by associated policies and procedures:

- **Acceptable Usage:** Users must utilize information systems responsibly and in accordance with authorized purposes.
- **Asset Management:** Assets must be identified, classified, tracked, and managed throughout their lifecycle.
- **Backup and Recovery:** Information must be regularly backed up, with restoration tests conducted at defined intervals.
- **Human Resource Security:** Employees must be screened, onboarded, and offboarded with due consideration to security roles and responsibilities.
- **Capacity Management:** IT resources must be monitored and planned to meet current and future business demands securely.
- **Monitoring and Logging:** Activities across systems must be logged, monitored, and reviewed periodically for anomalies.
- **Configuration Management:** All systems must adhere to secure baseline configurations and documented changes.
- **Cryptographic Controls:** Strong encryption techniques must be used for data in transit and at rest.

- **Data Privacy and Protection:** PII must be processed lawfully and securely, in line with DPDP requirements.
- **Governance and Audit:** A defined governance structure and audit program must ensure accountability and continual improvement.
- **Email Security**: Email systems must be secured against phishing, malware, and unauthorized access.
- **Information Classification:** Data must be classified and labeled based on sensitivity.
- **Retention and Disposal**: Information must be retained and disposed of in accordance with legal and business needs.
- **License Management**: Software use must be compliant with license terms and documented.
- **OS Security**: Operating systems must be hardened and updated regularly.
- **Mobile Device Security**: Mobile devices must be secured through MDM and acceptable use controls.
- **Access Control**: Access must be provisioned, reviewed, and revoked based on user roles.
- **Patch and VAPT**: Systems must undergo regular vulnerability assessments and timely patching.
- **Database Security**: Database platforms must be protected through configuration, access, and monitoring.
- **Vendor Security:** Third parties must be assessed for cybersecurity risks and contractual safeguards.
- **Project Security**: Information security must be embedded throughout the project lifecycle.
- **Password Controls:** Strong password policies must be enforced across systems.
- **Application Development**: Applications must be developed and tested using secure coding practices.
- **Physical & Environmental Security:** Physical access must be restricted, monitored, and reviewed.
- **Application Security:** Applications must be protected against OWASP Top 10 vulnerabilities.
- **Asset Disposal:** Obsolete assets must be securely wiped and decommissioned.

- **BYOD:** Personal devices must comply with security requirements before accessing corporate systems.
- **Change Management:** All changes must follow a documented, approved, and tested process.
- **Incident Management:** Incidents must be reported, analyzed, and mitigated within defined SLAs.
- **Threat Intelligence:** Emerging threats must be tracked and shared internally for proactive defense.
- **Network Security:** Network traffic must be segmented, encrypted, and protected against intrusion.
- **DLP & Malware Protection**: Tools must be implemented to prevent data loss and detect malicious code.
- **BCP & ITDR**: Business continuity and disaster recovery measures must be in place and tested periodically.

7 Reference

- SISL-IT-POL-Acceptable Usage Policy
- SISL-IT-POL-Asset Management Policy
- SISL-IT-POL-Backup And Restoration Policy
- SISL-IT-POL-Human Resource Security Policy
- SISL-IT-POL-Capacity Management Policy
- SISL-IT-POL-Log Management and Monitoring Policy
- SISL-IT-POL-Configuration Management Policy
- SISL-IT-POL-Cryptographic Control Policy
- SISL-IT-POL-Data Privacy Policy
- SISL-IT-POL-IT Governance and audit Policy
- SISL-IT-POL-Email Security Policy
- SISL-IT-POL-Information Classification Policy

- SISL-IT-POL-Information Archival, Retrieval & Deletion Policy
- SISL-IT-POL-Licence Management Policy
- SISL-IT-POL-Operating System Security Policy
- SISL-IT-POL-Mobile Computing Policy
- SISL-IT-POL-User Management & Access Control Policy
- SISL-IT-PRO-Patch Management and VAPT Policy
- SISL-IT-PRO-Database Security Policy
- SISL-IT-POL-Supplier Relationship Management Policy
- SISL-IT-POL-Project Management Policy
- SISL-IT-POL-Password Management Policy
- SISL-IT-POL-Secure Application Development Policy
- SISL-IT-POL-Physical and Environmental Security & Monitoring Policy
- SISL-IT-POL-Application Security Policy
- SISL-IT-POL-Asset Disposal Policy
- SISL-IT-POL-Bring your own device Policy
- SISL-IT-POL- Change Management Policy
- SISL-IT-POL-Incident Management Policy
- SISL-IT-POL-Threat Intelligence Policy
- SISL-IT-POL-Network Security Policy
- SISL-IT-POL-DLP & Malware Management Policy
- SISL-IT-POL-BCP & ITDR Policy

8 Policy Review Frequency

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

9 Policy Exception

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

10 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