SISL-IT-POL-Cyber Security and Cyber Resilience Policy

Version No: V 1.0

INTERNAL DOCUMENT

OCTOBER 2025

Document Control

Document Name	SISL-IT-POL-Cyber Security and Cyber Resilience Policy
Abstract	This document describes cyber security and cyber resiliency 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

Cyber threats to public, private, and government sectors continue to increase with the potential to cause widespread disruption to economic growth and stability, and national security. In order to address the need for the entire organization to contribute to a cyber-safe environment, the Cyber Security Policy highlights the risks from cyber threats and the measures to address / mitigate these risks.

2 Policy Statement

Appropriate technical and process controls shall be designed and implemented to protect the sensitive and critical data stored on Share India Capital Services Private Limited (SISL) information systems from cyber threats.

3 Scope

This policy applies to:

- All SISL information systems.
- All employees of SISL.
- All SISL owned Desktops/ Laptops / Mobile used by the employees of SISL
- All third Party personnel who work on SISL's premises or who remotely connect from
- their network to SISL's network

4 Roles and Responsibilities

Sr. No.	Role	Responsibility
1.	Designated Officer (DO)	Reviewer & owner
2.	Infosec Steering Committee	Recommend this policy for the approval of Board
3.	User (Employee / Contractor etc.)	▪ Read and understand the requirements of this policy and other policies referenced here. ▪ Follow the controls defined in this policy
5.	Information Technology Team	▪ Implement all technology controls on information systems.

		▪ Respond to cyber security incidents and provide RCAs.
6.	SOC (Security Operations Center)	▪ Monitor analyze and escalate security incidents ▪ Conduct Incident management and forensics analysis ▪ Coordination with stakeholders within / external. ▪ Develop response (As per Incident Management Policy) ▪ Generate cyber security dashboards.
7.	Incident Response Team	▪ Respond to Cyber incidents as per SISL policies. ▪ Update management and CMT on incident status. ▪ Perform RCA and take preventive actions.
8.	CMT (Crisis Management Team)	▪ Oversee the response to cyber incidents ▪ Provide critical decisions during the response cycle ▪ Manage external communications.

5 Overview and Governance

This policy focuses on cyber security activities and cyber security risks considered as part of SISL's risk management processes while meeting defined business objectives. This policy is a subset of information security policy and focuses on cyber security threats both internal and external impacting critical infrastructure of the organization. This policy will help the organization to align its cyber security activities with its vision, mission, and business goals.

5.1 Executive Level Oversight

SISL has one Executive level committees named Information Security Steering Committee (ISSC) to review Information Security and Cyber security activities. At least Half Yearly security updates on threat landscape and any major incidents across BFSI are discussed in these committee. This committee oversee the cyber security policy implementation and provide guidance on cyber security initiatives. The Cyber security policy shall be approved by the Board of Directors of SISL.

5.2 Information Security Steering Committee

The Information Security Steering Committee (ISSC) is chaired by the Chief Executive Officer (CEO) or/and top management and senior management and experts proficient in technology from various departments. The Committee oversees the on ground implementation of the controls and reviews the cyber security risks.

5.3 IT Team

The implementation of cyber security controls are coordinated by the information technology (IT) function led by the Head - IT. The Technology function coordinate with Operational risk function, Business units, and other support functions to ensure all cyber security related controls are implemented at their levels and risks are identified, reported and corrective actions taken.

5.4 Responsibilities

1. SISL payroll employees would have access to systems on basis of business needs and business unit head/HR approval.

2. SISL contract employees/ Vendor working for particular project will be tagged under particular business and basis of business head/ HR approval system access will be provided.

6 Standards and Guidelines

This policy outline controls in five broad categories namely Identify, Protect, Detect, Respond, and recover to effectively manage the cyber security event lifecycle.

6.1 Identify

These directives are foundational for understanding the business context, the resources that support critical functions, and the related cyber security risks to enable the organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.

6.1.1 Risk Identification

- SISL's mission, objectives, stakeholders, and activities shall be understood and used in risk assessments. The organization shall identify the cyber security risk to SISL's operations, its information assets, and individuals.
- The organization's priorities, constraints, risk tolerances, and compensating controls shall be considered to support risk acceptance decisions.
- Regulatory, legal, risk, environmental, and operational requirements for the organization shall be identified, monitored and managed. Applicable cyber security shall be considered during risk assessments and controls identification.
- Critical Business functions and their dependencies for delivery of critical services along with their respective resilience requirements shall be identified through Business Impact Analysis (BIA).

6.1.2 Asset Identification

- The data, devices, systems, software, business applications, personnel, services and facilities that enable the organization to achieve business purposes shall be identified and managed consistent with their relative importance to business objectives.

- All information assets shall have a designated owner. The owner has to be SISL employee and should be responsible to ensure data / information classifications and take reasonable measures to protect the asset.
- SISL shall prepare and maintain an up-to-date enterprise network architecture diagram.
- Cyber security requirements applicable for third party service providers shall be identified and communicated.
- Cyber security roles and responsibilities shall be identified and communicated to all stakeholders.

6.1.3 Vulnerabilities

- All information systems shall undergo security testing before inducting into the production environment and Yearly thereafter to identify critical vulnerabilities.
- SISL shall Yearly conduct application security testing for critical customer facing web/mobile applications throughout their lifecycle (pre-implementation, post implementation, after changes).
- All threats related to information assets, their respective vulnerabilities, potential impact and likelihood shall be identified, documented and used for risk assessment.
- Information systems backup and retention requirements shall be identified.

6.2 Protect

These section provides directives to develop and implement the appropriate safeguards to ensure secure delivery of critical infrastructure services. These controls supports the ability to limit or contain the impact of a potential cyber security event.

6.2.1 IT Architecture and Perimeter Security

- SISL's IT architecture shall be adequately designed, managed and controlled in order to ensure the required security controls are in place for protection of applications, infrastructure and information.
- SISL may implement solutions to automate network discovery and management.
- SISL shall implement security tools through defense in depth approach with perimeter security devices (e.g. Web gateway, IPS, Firewall etc.) and endpoint security tools to prevent and detect suspicious traffic.
- High availability mechanism (Clusters, RAIDs) and disaster recovery setup shall be implemented and aligned to approved RTO/RPO for critical business processes.
- Appropriate environmental controls shall be implemented for securing location of critical assets in line with "Physical Security Policy".
- List of authorized software shall be approved by Head - IT, which can be referred to install software on SISL's information systems.

6.2.2 Access Control

- Access to assets both physical and logical, shall be limited to authorized users, processes, or devices, and for authorized activities and transactions by principles of least privileges, separation of duties and/or through segregation of networks.
- Remote access to the information assets shall be restricted to authorized users and/or devices through authentication and secure communication channels.
- SISL shall implement centralized authentication and authorization system wherever possible for accessing and administering applications, operating systems, databases, network and security devices/systems, point of connectivity (local/remote, etc.) including enforcement of strong password policy, two-factor/multi-factor authentication depending on risk assessment and following the principle of least privileges and separation of duties.
- SISL shall implement appropriate systems and controls to allow, manage, log and monitor privileged/superuser/administrative access to critical systems (Servers/OS/DB, applications, network devices etc.).

6.2.3 Log Management

SISL shall manage the audit logs for critical information systems that includes but not limited to:

- identification of logs to be captured and frequency of log collection and storage;
- protecting logs from unauthorized modifications;
- analyze audit logs in a systematic manner so as to detect, understand or recover from an attack;
- perform forensic auditing if required;

6.2.4 Human Resource Security

- Adequate security practices related to human resources shall be implemented which may include but not limited to:
  a. Background screening of employees.
  b. Training of employees on their cyber security responsibilities.
  c. Access removal/modification in case of change of role or exit from SISL.
- Roles and responsibilities shall be clearly communicated to the SISL's personnel and partners. Targeted cyber security awareness education and shall be conducted, in line with the applicable policies; procedures; and agreements, to the stakeholders including but not limited to
  a. top management and Board;
  b. senior executives;
  c. information system users (employees and third party contractors);

d. physical security and information security personnel;

e. privilege users; and

- All stakeholders shall be made aware of SISL's cyber resilience objectives, and require and ensure appropriate action to support their synchronized implementation and testing.

6.2.5 Data Security

- Confidentiality, integrity, and availability of Customer's sensitive and personal information and records (data) shall be protected within SISL and with third party partners. Adequate controls shall be enforced to protect data throughout its lifecycle (i.e. origination, processing, storage, transmission, and disposal).
- Appropriate tools shall be implemented to monitor and prevent data leakage.
- Integrity of software, firmware, critical files, shall be monitored to detect any unauthorized modifications.

6.2.6 System Security

- Adequate controls shall be built to ensure that information security requirements are identified and implemented at each stage of system development life cycle from the requirement analysis till the disposal of the system. Systems used for development and testing shall be segregated from the production systems. Systems used for testing shall be a close replica of the respective production system.
- Secure configuration documents for operating systems, middleware, databases, mobile devices, network and security devices etc. shall be documented and used to manage protection of information systems and assets.
- SISL shall put in place patch management methodology. Systems and processes shall be implemented to identify, track, manage and monitor the status of applicable patches to Server operating Systems/Databases/Applications/ Middleware, etc.
- Remedial actions for identified risks and vulnerabilities shall be prioritized based on criticality of underlying asset and the potential impact of cyber security risk.
- The software installation/configuration change rights on all SISL information systems shall be restricted to authorized administrators only. Only authorized software shall be installed. Wherever feasible, consider implementing whitelisting of authorized applications/ software/libraries, etc. to prevent execution of unauthorized software and malicious code.
- Appropriate mechanisms shall be implemented to block/prevent and identify installation and running of unauthorized software / applications on end-user PCs, laptops, workstations, servers, mobile devices, etc.
- Appropriate mechanisms shall be implemented to identify authorized hardware / mobile devices like Laptops, mobile phones, tablets, etc. and ensure that they are provided connectivity only when they meet the security requirements prescribed by

SISL.

- All Changes to IT infrastructure and applications shall be reviewed and approved by respective application owner / appropriate authority as defined under SISL change management policy".
- Appropriate actions shall be taken to manage adequate capacity of information systems to ensure availability. The process may include but not limited to following:
  a. capacity predictions;
  b. defining thresholds;
  c. monitoring thresholds;
  d. augmenting capacity when thresholds are breached; and
  e. capacity reporting
- Maintenance and repairs of information system components shall be performed consistent with policies and procedures including:
  a. Maintenance and repair of organizational assets is performed in a timely manner
  b. Remote maintenance of organizational assets is approved and performed in a manner that prevents unauthorized access
- All enterprise mobile apps shall be rendered through mobile device management platform.

6.2.7 Backup and Removable Media

- Information systems backup shall be aligned to the identified backup and retention frequencies and monitored for adherence.
- Quarterly readability/Restoration testing shall be performed.
- Refer "SISL-IS-POL-007 - Media Sanitization and Disposal Policy" to control access to removable media that shall include but not limited to:
  a. Authorization for granting access
  b. Monitoring of data being copied
  c. Encrypting data
  d. Physical security
  e. Secure disposal

6.2.8 Protection Technologies

- Periodic (atleast Half Yearly) review of protection technologies and its configuration shall be carried out to evaluate the effectiveness of such technologies and cyber security controls.
- SISL shall evaluate new technologies for existing/evolving security threats before

adoption.

6.2.9 Risk Management

Requirements for justifying the exception(s), duration of exception(s), process of granting exceptions, and authority for approving, authority for review of exceptions granted on a periodic basis shall be documented.

6.3 Detect

This section provides directives to develop and implement the appropriate activities to timely discover the occurrence of cyber security event.

6.3.1 Detection Requirements

- Detection activities shall comply with all applicable requirements and may be tested Yearly (if feasible) and continuously improved.
- Detection processes shall be maintained and tested to ensure timely and adequate awareness of anomalous events.
- Any detected events shall be analyzed for potential impact and severity rating shall be assigned.
- All detected events shall be timely reported to the appropriate resolver groups.

6.3.2 Security Operations Center

- A 24 x 7 centralized security operations center shall be institutionalized to timely detect and analyze anomalous activity and ascertain potential impact of events across critical systems.
    a. A baseline of network operations and expected data flows for users and systems shall be established and managed
    b. Event data shall be aggregated and correlated from multiple sources and sensors
    c. All security event correlation shall be monitored to detect any cyber security event.
    d. Detected events shall be analyzed near real time for infrastructure and applications to understand attack targets and methods, appropriate alert thresholds shall be established.
- Following monitoring activities shall be performed at the minimum to identify cyber security events and verify the effectiveness of protective measures.
    a. The network traffic anomalies
    b. The physical environment
    c. Privilege user activities
    d. Endpoint systems to identify malware and violation of acceptable usage policy.
    e. Fake mobile applications, Phishing sites, malware monitoring on internet facing systems, and Trojan monitoring

f. Unauthorized personnel, connections, devices, and software.

6.3.3 Physical monitoring

- Adequate physical and environmental controls shall be implemented and monitored to protect critical assets of SISL with respect to temperature, water, smoke, access alarms, service availability alerts (power supply, telecommunication, servers), access logs, etc.
- Roles and responsibilities for detection shall be well defined to ensure accountability
- Event detection information shall communicated to appropriate parties
- Onsite audits may be conducted for external service provider to ensure compliance with SISL's security requirements and detect any cyber security risks.
- End users shall report any actual or suspected cyber security incidents to SISLINFOSEC@shareindia.co.in.

6.4 Response

This section defines directives to implement appropriate activities to take action regarding a detected cyber security event and enables SISL employees and support / outsourced staff to contain the impact of a potential cyber security event.

6.4.1 Identifying and rating Cybersecurity Incident

- The prompt response mechanism shall be in place
- The prompt response mechanism shall be in place for at least following types of cyber security incidents:
  a. successful or failed attempts to intrude SISL's network;
  b. major virus outbreak or zero day attack;
  c. data Theft by Internal or external entity;
  d. major denial attack against SISL network (DoS / DDoS);
  e. Ransom-ware and other advanced persistent threats;
  f. identity theft attacks;
  g. successful malicious call back traffic;
  h. website defacement;
  i. misuse / inappropriate use of system;
  j. critical system outage due to above vectors
- Criteria shall be decided on rating cyber security incidents.

6.4.2 Incident Response

- Cyber Crisis Management plan, approved, by Security Council shall be put in place to

ensure

a. effective and orderly response to detected cyber security incidents;

b. minimize loss or theft of information and disruption of service;

c. to gain learnings and create knowledgebase for better handling future incidents;

d. dealing properly with legal requirements; and

e. appropriate escalation and communication to stakeholders

- Crisis Management team (CMT) shall be constituted which shall analyze and respond to cyber security incidents and coordinate activities related to the incident containment and resolution.
- Roles and responsibilities of the Crisis Management teams (CMT) shall be documented and communicated to the team.
- SISL shall document incident response procedures including the roles of staff / outsourced staff handling such incidents.
- SISL if required may empanel partners for network forensics/forensic investigation services.
- The Designated Officer of the Member shall continue to report any unusual activities and events, all Cyber-attacks, threats, cyber-incidents and breaches experienced by Members to NSE (in manner specified by NSE) & SEBI (on the dedicated email ID: mkt_incidents@sebi.gov.in) within 6 hours of noticing / detecting such incidents or being brought to the notice about such incidents as well as submit the quarterly reports containing the information on cyber-attacks, threats, cyber-incidents and breaches experienced by Stock Brokers and measures taken to mitigate vulnerabilities, threats and attacks including information on bugs / vulnerabilities, threats that may be useful for other Stock Brokers / Depository Participants / Exchanges / Depositories and SEBI shall be submitted to Stock Exchanges within 15 days after the end of the respective quarter in the manner as specified by NSE from time to time.
- Members shall report the Cyber Security incident to Indian Computer Emergency Response Team (CERT-In) in accordance with the guidelines / directions issued by CERT-In from time to time. Additionally, the Members, whose systems have been identified as “Protected system” by National Critical Information Infrastructure Protection Centre (NCIIPC) shall also report the incident to NCIIPC.

6.5 Recover

This section defines directives to establish and maintain plans for resilience and to restore any capabilities or services that may have been impaired due to cyber security event and timely recovery to normal operations.

- Recovery processes and procedures shall be executed and maintained to ensure timely restoration of systems or assets affected by cyber security events
- Recovery planning and processes shall be improved by incorporating lessons learned into future activities

- Restoration activities shall be coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, attackers (if applicable), victims, CERT-IN, and vendors. Additionally,
  a. public relations shall be managed;
  b. reputation after an event shall be repaired;
  c. recovery activities shall be communicated to internal stakeholders and executive and management teams
- SISL if required may align Security Operation Centre, Incident Response and Digital forensics to reduce the business downtime/ to bounce back to normalcy

7 Reference

Ref: SISL-IT-PRO- Backup and restoration procedure

8 Policy Review Frequency

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