Share India
You generate, we multiply

SISL-IT-POL-Physical and Environmental Security Policy

Version No: V 1.0

INTERNAL DOCUMENT

OCTOBER 2025

Document Control

Document Name	SISL-IT-POL-Physical and Environmental Security Policy
Abstract	This document describes physical and environmental 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

Access control is a mechanism to ensure that authorized personnel have access to the information and information processing resources that are assigned to them.

Physical protection of sites that house the critical information assets is important so as to prevent unauthorized access. Improper or Inadequate physical access control mechanism may lead to loss of critical equipment's and data.

2 Policy Statement

To provide and ensure controlled physical access and environmental security to information and information system assets in line with the business and information security requirements. Access control ensures that only authorized personnel have access to the information or information processing facilities.

3 Scope

This policy applies to

- All locations where users have access to various information assets including locations that have secure areas hosting critical information assets.
- All information assets including data, applications, network devices, security devices, servers, smart phones and other IT systems that need adequate physical and environmental protection.
- All the employees of SISL.
- All third-party vendors working in SISL premise.

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.	Department Heads	Identify access rights to be granted to the users. Ensure that all users are aware of this policy
4.	Admin Team	Ensure that the Physical and Environmental concerns are addressed, and premises is monitored.
5.	IT Team	Ensure that the Physical and Environmental concerns are addressed for all IT assets

5 Physical Access Policy

5.1 Physical Perimeter Security

Physical access to the premise shall be protected and only authorised users shall be given access to the premise.

5.2 Entry Restrictions for Employees

Entry to various security zones shall be restricted based on the role of the personnel within the organization. The restriction shall be enforced through the use of biometric control mechanism.

The information security team shall be informed of any abnormal events.

Employees for whom biometric access to the premise has not been enabled shall ensure that their access has been enabled by Admin. All Employees of SISL shall display their identity cards while in the office premises.

Access rights granted to employees and vendors shall be reviewed monthly.

5.3 Entry Restriction for Visitors

Visitors shall be restricted to the reception area only. The concerned employee shall be intimated, and he/she shall escort the visitor on premises at all times. Visitor book shall be maintained for all visitors, this record shall be preserved and reviewed periodically or in case of an incident.

5.4 Physical access to the server room

- Physical access to server room shall be restricted to authorised persons only. The Information Security Manager shall authorize the access. Information Security Team shall review the accesses granted to the various personnel on a monthly basis.
- Vendors requiring access to the server room for maintenance work shall be accompanied by authorized person and all the work shall be done under their supervision. No third party shall have access to the server rack unless supervised by the authorized personnel at all times during the stay.
- The Information Security Manager shall be authorized to revoke the access rights of an employee to the server room.
- The server room shall be always locked.
- Access to the server room shall be reviewed quarterly jointly by admin and local IT.

5.5 Physical Security of all assets

Department Heads shall be responsible for the physical security of desktops allotted to their team and shall be responsible for ensuring the physical security of all the assets. The respective users shall protect physical asset against fire, water and pollution damage. They shall be responsible to ensure safety of the assets allocated to them and shall inform the IT department in case any event is noted.

Regular maintenance and servicing of the asset shall be done as per the AMC or on a contractual basis.

Physical assets shall include but not be limited to assets like desktops, laptops, handheld devices, Network equipment's, faxes, printers, LCD panel, telephones, fire extinguishers, fire panel, smoke detectors, and photocopiers wherever applicable which are managed and maintained by SISL.

5.6 Cabling Security

Cables carrying data or supporting information services shall be protected from interception or damage. Power and telecommunications lines within the premises shall be adequately protected from physical damage. Network cabling shall be protected from unauthorized interception or damage, by using conduits. Power cables shall be segregated from communications cables to prevent interference. The network switches located throughout the premises shall be placed in locked cabinets and shall be protected from fire, heat, dust and water.

5.7 Clean Desk & Clear Screen

The following controls shall be implemented for all the users

- Paper used during work hours shall be either locked away in the lockers or be shredded at the end of the day.
- Paper and computer media shall be stored in suitable locked cabinets and/or other forms of secured area when not in use and after office hours.
- Sensitive or critical business information shall be locked away (ideally in a fire-resistant safe or cabinet) when not required, especially when the office is vacated. Personal computers, computer terminals and printers shall not be left logged on when unattended. The terminal should be locked in such cases. Wherever applicable, the terminals, servers, user systems shall timeout and the screen cleared automatically if the terminal is inactive for more than 15 minutes.
- Photocopiers if required shall be locked (or protected from unauthorized use in some other way) outside normal working hours.
- Sensitive or classified information, when printed, will be cleared from printers immediately.

5.8 Handling of Storage Media and other Equipment

5.8.1 Handling of Data Storage Media

- The data storage media shall be stored in proper atmospheric conditions to reduce deterioration because of atmospheric condition variance and for ready availability.
- Data storage media packs shall be stored in a safe and cool location.
- Data storage media shall not be exposed to direct sunlight.

- Data storage media packs shall be properly labelled.
- All external storage media like pen-drives if used anytime with authorisation at SISL and the media does not belong to SISL shall be checked for on a designated PC before being used on the machines. Any virus detected shall be cleaned before the external storage device is released. Virus software shall also reside on the PCs connected to the network as well as stand-alone PCs. The virus software shall be upgraded regularly as per the antivirus policy.

5.8.2 Handling of other Equipment

- Magnetic material shall not be brought into the computer area without the prior permission of designated individual/s.
- Movement of equipment shall be recorded for control on physical inventory.
- System units, PC's and peripherals shall be regularly maintained to ensure uninterrupted usage.

6 Physical Security Monitoring

SISL shall ensure that premises is continuously monitored for unauthorized physical access to detect and deter any unauthorized physical access.

6.1 Monitoring Guidelines

Physical premises shall be monitored by surveillance systems, which can include guards, intruder alarms, video monitoring systems such as closed-circuit television and physical security information management software either managed internally or by a monitoring service provider.

Access to buildings that house critical systems shall be continuously monitored to detect unauthorized access or suspicious behaviour by:

- Video monitoring systems such as closed-circuit television to view and record access to sensitive areas within and outside an organization's premises.

The design of monitoring systems shall be kept confidential, as disclosure can facilitate undetected break-ins. Monitoring systems shall be protected from unauthorized access to prevent surveillance information, such as video feeds, from being accessed by unauthorized persons or systems being disabled remotely.

The alarm system control panel shall be placed in an alarmed zone and, for safety alarms, in a place that allows an easy exit route for the person who sets the alarm. The control panel and the detectors shall have tamperproof mechanisms.

The system shall regularly be tested to ensure that it is operational as intended, particularly if its components are battery powered.

7 Reference

7.1 Fire Damage

7.1.1 Firefighting equipment (Fire alarm and smoke detectors)

- Fire extinguishers shall be used and placed in SISL work area and at an easily accessible location of the premises.
- Fire alarms and smoke detectors shall automatically trigger the alarms in case of smoke/ fire outage.
- The smoke detectors shall detect and highlight the floor and section that triggered the smoke detector alarm. This information shall be used by the fire wardens to quickly proceed to the exact location that triggered the alarm.
- This information shall be available with the fire wardens and with the administration department.
- Emergency contact numbers shall be visibly placed within the SISL premise (at prominent places)

7.2 Water Damage

- Wherever possible the ceiling and the walls of the building shall be adequately coated with chemicals to prevent seepage of water.
- Water and other liquids shall not be allowed in the server rooms as machines and cables could get damaged due to spillage.
- The drainage system shall be in a way such that water pipes are placed away from the user work areas and server rooms.

7.3 Electrical Damage

7.3.1 Electrical fittings

- An overall diagram of the electrical layout of the work area shall be prepared to identify all electrical points.
- The air conditioning system shall be effective and the temperature in the SISL work area shall be monitored regularly.
- The server room shall be equipped with temperature monitoring devices, and it shall be ensured that the temperature is always maintained below 20 degrees Celsius. Air conditioning shall be available on a 24*7*365 basis.

7.3.2 Power Supply

- Power to computer systems shall be through uninterruptible power system (UPS). It shall be ensured that the UPS is always in working condition. In case laptops are used, UPS may be eliminated at that location.

- Voltage regulators shall be installed to guard against fluctuations in power.
- Circuit breakers of appropriate capacity shall be installed to protect the hardware against increase in power voltage.
- Earthing to system and networking equipment's shall be from separate dedicated earth pits. Voltages to all crucial equipment's shall be monitored during the preventive maintenance activity of the UPS.
- Generators shall be provided for the generation of power in case of failure of the general power lines in locations susceptible to power fluctuations.
- Above security systems shall be tested during the preventive maintenance round of the UPS.

7.3.3 Protection of power lines supporting IT services and telecommunications

- All cables carrying data and power supporting IT services shall be protected from unauthorized tapping or disruption. Careful consideration in location and accessibility shall be taken when running wires.

7.4 Pollution Damage

- Regular cleaning of the floor, walls, storage cabinets and IT equipment is necessary.
- Dust generating activities e.g. paper shredding should be carried out away from the work area.

8 Incident Management

Any physical and environmental breach shall be logged as an incident and shall be in compliance with the Incident Management Policy.

9 Change Management

Any changes to the physical and environmental security controls shall be made as per the Change Management Policy.

10 Reference

Ref: SISL-IT-POL-User Management and Access Control Policy

11 Policy Review Frequency

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

12 Policy Exception

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

13 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