SISL-IT-POL-Mobile Computing Policy

Version No: V 1.0

INTERNAL DOCUMENT

OCTOBER 2025

Document Control

Document Name	SISL-IT-POL-Mobile Computing Policy
Abstract	This document describes mobile computing 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

Laptops, have become thief magnets, attracting everything from common thugs to sophisticated conmen, hi-tech crime rings and industrial spies. These devices tend to contain data that can cause a lot of damage if it falls into the wrong hands, not to mention the monetary loss in terms of the cost of the device.

Similarly wireless handheld Portable Electronic Devices (PED), such as tablets, smart phones etc enable mobile ad-hoc networking of the workforce and provide flexible data access and electronic-commerce capabilities. These days such PED's increasingly retain corporate information, but unlike their desktop counterparts, they lie at the periphery of organizational controls and oversight. Limited computing power, memory, interfaces, and battery life impose constraints on the practicality of applying standard safeguards. The PED's small size and mobility also leads to greater exposure to theft or misuse in the field.

2 Policy Statement

This policy has been framed to protect Share India Securities Limited's (SISL) capital investment and information assets specifically used for mobile computing.

3 Scope

This policy applies to

- All the employees of SISL
- Smart phones and PEDs
- Laptops
- Tablet PC's

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 Team	AV installation, device management, data encryption
4.	Human Resource	Ensure that all SISL employees are aware of this policy

5.	Users	Shall abide by this policy

5 Standards and Guidelines

5.1 Laptop Security

5.1.1 Asset Identification

The laptop shall be tagged appropriately as per the company's tagging methods

The following details shall be maintained in an asset register

- Laptops model no.
- Laptops Serial No. &
- Laptops purchase details

5.1.2 Identification of OS services and Security needs

The IT Team shall identify the services required on the laptop and security requirements for the laptop. These requirements shall be documented and approved by the Information Security Manager.

5.1.3 Installation

The IT department shall ensure that the following have been completed –

- All OS and application related patches have been applied on the laptop
- All security requirements as identified have been configured.
- Anti-virus software is installed on the system.
- Access is provided as per the identified requirements.

5.1.4 Treatment of default accounts and groups

The operating system often includes default accounts and passwords. The IT Teams shall ensure the following

- Guest accounts shall be disabled.
- Administrator user account shall be disabled wherever possible or separated account with administrative privileges shall be created and used.
- Default users accounts generated by the operating system or installed applications shall be disabled if they are not in use.

5.1.5 Network Security

The Bluetooth can be used to transmit data and can also be used to browse the files on a laptop without the user's knowledge. This vulnerability is often overlooked. The Bluetooth on

SISL's laptops shall be disabled, if not required. In case of a business requirement to let these ports remain open, these shall be monitored for unauthorized access using DLP.

It shall be ensured that adequate security measures are provided so as to facilitate secure use of the Wi-Fi connectivity. The following shall be done –

- Harden the operating system
- Use adequate password authentication
- Run a firewall and adware / spyware removal tools if required

5.1.6 USB ports

USB ports can be used for connecting various devices like – keyboards, scanners, mouse, printers, flash disks, digital cameras etc. Devices like flash disks and digital cameras can be used to store and transfer information.

To ensure that no unauthorized person transfers information using any I/O devices that can connect to the USB port, SISL shall disable the USB port.

Authorized users will be granted USB access upon providing a valid business justification. The IT Infrastructure team shall maintain a list of authorized users.

5.1.7 Data Security

As a company policy the laptop shall not hold any business-critical information. This information shall be maintained on identified servers / portals. However, in case the laptop does carry critical business data, then the laptop owner shall ensure that this data is encrypted.

5.1.8 Physical Security

The physical security of the laptop is the responsibility of the user to whom the laptop has been allocated. It is the responsibility of the concerned user to follow and abide by the laptop guidelines. It is the responsibility of the concerned user to read and understand these guidelines.

5.1.9 Data Backup

Data on the laptop is more expensive to replace than the hardware. If the user is traveling for an extended period of time, the data on the laptop shall be backed up. The concerned user shall contact the IT administrator to back up the laptop data.

5.1.10 Logging / Auditing

The IT Team shall configure the laptop to log successful and failed login attempts. On critical laptops, activity auditing shall be enabled to track.

- Successful and rejected system access attempts.
- Successful and rejected data and other resource access attempts.

- Access and modification of critical files.

5.1.11 Monitoring

All the data residing on the laptops is the property of the company. SISL reserves the right to install any monitoring software on the laptops and the right to monitor the company laptops for any inappropriate, abusive or unethical use. Employees conducting any inappropriate, abusive or unethical use of the laptops can be held responsible and legal and / or punitive action shall be taken against them. All communications, including text and images, done using the laptops can be disclosed to law enforcement or other third parties without prior consent of the sender or the receiver.

5.2 Portable Electronic Device (PED)

Portable Electronic Devices (PEDs) such as smart phones etc. allow users to synchronize personal databases as well as official data and provide access to network services such as wireless e-mail, Web browsing, and Internet access. All of these devices can be used to transport data surreptitiously to be read / decoded at a later time. Hence while using smart phones etc. provided by SISL users shall ensure that business information is not compromised, and unethical use of these devices is not carried out.

5.2.1 Data Security

Where appropriate and possible, the IT Department of SISL shall meet with the following requirements for the PEDs

- Access controls – Access controls shall be granted as per business requirement and need to know basis only. Remote access to business information across public network using mobile computing facilities shall only take place after successful identification and authentication, and with suitable access control mechanisms in place.
- Cryptographic techniques – Where appropriate and possible the data contained on these devices shall be encrypted.
- Back-ups - Back-ups of critical business information residing on these devices shall be taken regularly. Equipment shall be available to enable the quick and easy back-up of information. These back-ups shall be given adequate protection against, e.g., theft or loss of information.
- Virus protection – Where appropriate and possible, protection shall be provided employing anti-virus software.

5.2.2 Physical Security

The respective users shall be responsible for the physical security of the device. The concerned user shall take care to ensure that

- PED is physically protected against theft especially in cars and other forms of transport, hotel rooms, conference centers and meeting places.

- PEDs carrying important, sensitive, and/or critical business information shall not be left unattended.
- The IT Team shall properly tag these assets and maintain an updated asset register that includes all the PEDs.

5.3 Disciplinary action

This policy shall be strictly followed by all employees of SISL using its laptops / PED's. Any breach, whether intentional or unintentional, shall be viewed seriously by SISL. SISL reserves the right to take necessary disciplinary action against the employee in breach of this policy. Depending upon the seriousness of the breach, SISL may, in its sole discretion, decide upon the type of disciplinary action which may include summary dismissal without notice.

5.4 Theft Insurance

The laptop shall be insured against theft with the Insurance Company as necessary. It shall be ensured that the company covers theft regardless of where it happens.

SISL shall take into account legal, insurance and other security requirements for cases of theft or loss of the PEDs.

5.5 Incident Management

In case of any breach, the same shall be logged in the Incident Report and a proper incident management process shall be followed in compliance to SISL's Incident Management Policy.

5.6 Change Management

Any changes shall be done as per SISL's Change Management Policy.

6 Reference

Ref: SISL-IT-PRO- Asset 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