SISL-IT-POL-Bring your Own Device Policy

Version No: V 1.0

INTERNAL DOCUMENT

OCTOBER 2025

Document Control

Document Name	SISL-IT-POL-Bring your own Device Policy
Abstract	This document describes BYOD Policy 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 4

2 Policy Statement 4

3 Scope 4

4 Roles and Responsibilities 5

5 Standards and Guidelines 5

5.1 Policy axioms (guiding principles) 6

5.2 Devices and Support 6

5.3 Reimbursement 6

5.4 Device Security Controls 6

5.5 Risks / Liabilities / Disclaimers 8

5.6 Incident Management 8

6 Policy Review Frequency 8

7 Policy Exception 8

8 Policy Violation Reporting Matrix 9

1 Introduction

Personally Owned Devices (PODs) such as smart phones, tablets, laptops etc. allow users to synchronize personal as well as official data and provide access to network services such as Email and Internet access. All these devices can be used to transport data surreptitiously to be read / decoded at a later time. Hence while using PODs, the user shall ensure that business information is not compromised, and unethical use of these devices is not carried out.

Share India Securities Limited (SISL) grants its employees and relevant interested parties the privilege of using personal smartphones and laptops of their choice for work related at SISL for their convenience. SISL reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below.

This policy is intended to protect the security and integrity of SISL's data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms.

SISL employees and relevant interested parties shall agree to the terms and conditions set forth in this policy in order to be able to connect their personal devices to the company network. (Currently only for senior management/authorized users)

2 Policy Statement

Employees and relevant interested parties who are authorized to use their personally owned smartphone, laptops for work purposes shall secure corporate data to the same extent as on corporate IT equipment and shall not introduce unacceptable risks (such as malware) onto the corporate networks by failing to secure their own smartphone/equipment.

3 Scope

This policy forms part of the corporate governance framework. The policy is applicable to

- Employees and relevant interested parties, who are authorized to use personal owned devices for work purposes.
- Third party acting in a similar capacity to our employees and relevant interested parties whether they are explicitly bound (e.g. by contractual terms and conditions) or implicitly bound (e.g. by generally held standards of ethics and acceptable behavior) to comply with our information security policies.
- Clients who connect to the IT infrastructure are supported by SISL.

4 Roles and Responsibilities

Sr. No.	Role	Responsibility
1.	Designated Officer (DO)	Ensure that this policy is effectively implemented.
2.	IT infrastructure Team	AV installation, device management, data encryption
3.	Human Resource	Ensure that all SISL employees and relevant interested parties are aware of this policy
4.	Users / Contractors/ Relevant Interested Parties	Shall abide by this policy

5 Standards and Guidelines

In contrast to Information and Communications Technology (ICT) devices owned by the organization, Personally Owned Devices (PODs) are ICT devices owned by employees or by third parties (such as suppliers, consultants and maintenance contractors). Authorized employees and third parties may wish to use their PODs for work purposes, for example making and receiving work phone calls and text messages on their own personal cellphones, using their own tablet computers to access, read and respond to work emails, or working in a home-office.

Bring Your Own Device (BYOD) is associated with a number of information security risks such as:

- Loss, disclosure or corruption of corporate data on PODs
- Incidents involving threats to, or compromise of, the corporate ICT infrastructure and other information assets (e.g. malware infection or hacking)
- Noncompliance with applicable laws, regulations and obligations (e.g. privacy or piracy)
- Intellectual property rights for corporate information created, stored, processed or communicated on PODs in the course of work for the organization.

Due to management's concerns about information security risks associated with BYOD, individuals who wish to opt-in to BYOD shall be authorized by management and shall explicitly accept the requirements laid out in this policy beforehand.

Management reserves the right not to authorize individuals, or to withdraw the authorization, if they deem BYOD not to be appropriate and in the best interests of the organization.

5.1 Policy axioms (guiding principles)

- The organization and the owners and users of PODs share responsibilities for information security.
- Nothing in this policy affects the organization's ownership of corporate information, including all work-related intellectual property created in the course of work on PODs.

5.2 Devices and Support

- Smart phones including iPhone, Android phones shall be allowed.
- Employees and relevant interested parties shall contact the device manufacturer or their carrier for operating system or hardware-related issues.
- Devices shall be presented to IT for proper job provisioning and configuration of standard apps like email, office productivity software and security tools, before they can access SISL services.

5.3 Reimbursement

- The company shall not reimburse the employee the cost of the device.
- The company shall not
    - Pay the employee an allowance.
    - Cover the cost of the voice/data plan.
    - Roaming, plan overages, etc.

5.4 Device Security Controls

5.4.1 Data Security

Where appropriate and possible, the IT Department shall ensure that the following requirements are compiled to –

- Password Protection - In order to prevent unauthorized access, devices shall be password protected using the features of the device and a strong password is required to access the company network. The device shall lock itself with a password or PIN if it's idle for 15 minutes.
- Access controls – Access controls shall be granted as per business requirement and need to know basis only. Remote access to business information across public networks using PODs shall 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. Any POD used to access, store or process sensitive information shall encrypt data.
    - Transferred over the network (e.g. using SSL or a VPN)
    - While stored on the POD or on separate storage media (e.g. MDM),

- Rooted (Android) or jail-broken (iOS) devices are strictly forbidden from accessing the network.

- The employee's device may be remotely wiped if.
    - The device is lost.
    - The employee terminates his or her employment.
    - IT detects a data or policy breach, a virus or similar threat to the security of the company's data and technology infrastructure.
- Since the IT team does not have the resources or expertise to support all possible devices and software, PODs used for BYOD shall receive limited support on a 'best endeavors' basis for business purposes only.

- While employees and relevant interested parties have a reasonable expectation of privacy over their personal information on their own equipment, the organization's right to control its data and manage PODs may occasionally result in support personnel unintentionally gaining access to their personal information. To reduce the possibility of such disclosure, POD users are advised to keep their personal data separate from business data on the POD in separate directories.

- Take care not to infringe other people's privacy rights, for example do not use PODs to make audio-visual recordings at work.

5.4.2 Physical Security

The POD owner shall be responsible for the physical security of the device. The concerned user shall take care to ensure that –

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

- PODs carrying important, sensitive, and/or critical business information shall not be left unattended.

5.5 Risks / Liabilities / Disclaimers

- IT shall take every precaution to prevent the company data from being lost, in the event it must remotely wipe a device, it is the employee's responsibility to take additional precautions, such as backing up email, contacts and employee's personnel data, etc.
- SISL reserves the right to disconnect devices or disable services without notification.
- Lost or stolen devices shall be reported to the company within 24 hours. Employees and relevant interested parties are responsible for notifying their mobile carrier immediately upon loss of a device.
- The employee shall be expected to use his or her devices in an ethical manner at all times and adhere to the company's acceptable use policy.
- The employee shall be personally liable for all costs associated with his or her device.
- The employee shall assume full liability for risks including, but not limited to, the partial or complete loss of company and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.
- SISL reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.

5.6 Incident Management

In case of a security breach through the use of a POD, an incident will be logged in the Incident Management tool and the incident shall be addressed in line with SISL's Incident Management Policy.

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