Share India
You generate, we multiply

SISL-IT-POL-License Management Policy

Version No: V 1.0

INTERNAL DOCUMENT

OCTOBER 2025

Document Control

Document Name	SISL-IT-POL-License Management Policy
Abstract	This document describes license management 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

Share India Securities Limited (SISL) utilizes open-source applications, operating systems and databases to enable their business functions. Being open source, most of these IT enablers are available under the open-source license agreement. However, Windows Operating systems, certain office automation tools like Microsoft Office etc., are license based.

2 Policy Statement

The License Management Policy has been framed to ensure that SISL manages all their software licenses as per their license agreement with the software vendors.

3 Scope

The policy applies to

- All the software being used / owned by SISL
- The IT / Infrastructure team
- The Development team

4 Roles and Responsibilities

Sr. No.	Role	Responsibility
1.	Designated Officer (DO)	Ensure that this policy is implemented
2.	Information Security Manager (ISM) & Business Operations	Monitor and control the use of software
3.	IT / Infrastructure Team	Installation, un-installation, monitor software usage as per the policy
4.	Human Resource	Ensure that all employees are aware of this policy
5.	All Employees	Shall not install any unlicensed software

5 Standards and Guidelines

SISL shall maintain a track of all software installed on the servers, workstations and laptops.

5.1 Software Inventory

SISL shall have a centralized system to keep track of all software installed on their servers / workstations. The IT / Infrastructure team shall be responsible for the maintenance of this inventory.

The IT team shall maintain a log of the installation and un-installation of all evaluation software used at SISL.

5.2 License Management Process

5.2.1 Software Installation / un-installation

All licensed software installation or un-installations shall be done by the IT Team only.

The IT Team shall have a checklist of the minimum software to be installed on a user's PC. This shall help them set up the system for a user, as per the department's requirement.

Any user with a need for additional licensed software to be installed on their PC shall obtain approval for the same and then work with the IT Team to install the software.

5.2.2 Authorization for Installation

5.2.2.1 Productivity software

Productivity software is defined as the software that is used for carrying out day-to-day activities, such as managing documents, network management, system administration, accounting etc.

The IT Team shall install the required software as per the department's requirements. In case a user requires additional licensed software, the request for the same shall be routed through their department head. The department head shall forward the request to the Information Security Manager who shall verify the license availability for the requested software and then inform the IT Team to do the needful.

If the license is not available, the Information Security Manager shall inform the requesting department head of the same. If the department head agrees to the purchase of the software, the concerned department will be involved in the purchase process. After the software is purchased, the Information Security Manager shall notify the IT Team to install the software on the user's computer.

5.2.2.2 Trial Ware / Evaluation Software

Trialware or evaluation software allows the user to test its functionality for a limited period of time. Employees who need evaluation software installed on their PCs, shall get permission from their Head of Department prior to downloading the software. This authorization shall then be forwarded to the Information Security Manager who shall forward this request to the IT Team for further action. After the evaluation period is over, the user shall uninstall the evaluation software from the user's PC.

The IT Team shall maintain a track of all evaluation software that has been installed or un-installed on the servers / workstations of SISL.

Employees shall not use 'cracks' to try and unlock the evaluation software.

5.2.2.3 Installation of freeware/community edition

Freeware / community edition software is available free of cost from the Internet or from the CDs accompanying periodicals or computer books. Such software can aid productivity; however, one needs to exercise caution before installing any Freeware / community edition.

The IT Team shall test any Freeware / community edition required to be installed on servers / workstations of SISL. A separate test machine shall be used for carrying out critical tests. The minimum tests that shall be carried out are –

- Ensure that the Freeware / community edition does not load any spy ware / Trojans.
- Check the ports that are opened when the software is used.
- Ensure that system stability is not affected by the use of the Freeware / community edition.

Employees, with requirement of Freeware / community edition installation on their PCs, shall first get the permission from their respective Head of Department. The Head of Department shall inform the Information Security Manager who shall in turn instruct the IT Team about the request.

The IT Team shall download and install critical software after testing it as mentioned above.

If the test results indicate that the software is safe to use, then the Information Security Manager shall authorize the IT Team to install the software. Else the request to install the software is revoked.

5.3 Software Copies

The IT Team is permitted to make a copy of licensed/ evaluation software CD, Software that is downloaded from the Internet etc. No employee shall make unauthorized copies of any software.

5.4 Storage of licenses

The License documents, copyrights agreements and the software media shall be placed in a secured location or folders. Access to this location or folders shall be restricted to the IT Team and Information Security Manager only.

5.5 Monitoring

The IT Team shall monitor all servers and workstations for the software that is installed on them. Any software found to be installed without proper authorization shall be immediately uninstalled.

5.6 Software Disposal / Decommissioning

A software may have reached its usefulness period and may require to be disposed. In such a case, the IT Team shall work with the various departments to check their software requirement needs.

A software shall be decommissioned when it has become obsolete, a newer version has been released by the vendor, SISL has decided to move to another better software / platform etc.

In any of these cases, the software decommissioning shall be done after an approval has been obtained from the Information Security Officer. The software disposal shall be in any form such as a buy back by the vendor or a discontinuation of the software usage.

The IT Team shall ensure that this software is no longer available in their software repository. A copy of the same may be maintained on an external media and stored in a safe location. Access to the same shall be restricted. All manuals /documents related to the software shall be destroyed. The licenses shall be retained but marked as decommissioned.

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