SISL-IT-POL-Asset Management Policy

Version No: V 1.0

INTERNAL DOCUMENT

OCTOBER 2025

Document Control

Document Name	SISL-IT-POL-Asset Disposal Policy
Abstract	This document describes Asset disposal 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

Information can be compromised through careless disposal or re-use of IT assets. Storage devices containing sensitive information shall be physically destroyed or securely overwritten.

2 Policy Statement

Share India Securities Limited (SISL) shall ensure that all the assets owned by them containing data and licensed software shall be reliably erased and the media destroyed reliably as per industry's best practice.

All storage media shall be checked prior to disposal to ensure that sensitive data and licensed software's are removed or overwritten.

3 Scope

The policy applies to

- All the hardware assets within the office premise
- All assets hosted in the server room
- All employees of SISL
- All electronic or paper media holding information

4 Roles and Responsibilities

Sr. No.	Role	Responsibility
1.	Designated Officer (DO)	Ensure that the policy is implemented
2.	Information Security Manager (ISM)	Enforce the policy
3.	IT Team	Implement and abide by the policy
4.	Users and Suppliers	Abide by the policy

5 Standards and Guidelines

5.1 Asset Disposal Criteria

The assets shall be disposed of under the following conditions.

- No economic benefits derived from the active use of the asset.
- Maintenance cost of the asset exceeds its replacement value.
- Upgradation of the asset is not feasible.
- Replacement or disposal reduces the cost of operations and improves efficiency.
- Asset is no longer optimally used due to technology and market dynamics.
- Asset condition
- Asset has served its value to the organization.

5.2 Disposal Authorization

Proper authorization shall be obtained prior to the disposal activity.

- The Information owner shall sign off the authorization for media disposal and mark the media for disposal.
- The information owner shall schedule the pickup of items marked for disposal or formally transfer the item to the concerned department for disposal.
- Media (paper, CD-ROMs, hard disk, external storage devices, USB pen drives, and smart phones) can be disposed of within the premises.
- The disposal area shall be physically secured with access to authorized personnel only.
- Confidential data shall be disposed of at a smaller frequency cycle as compared to other assets.

Any disposal of electronic media shall comply with environmental

5.3 Disposal of paper assets

The department heads shall be responsible for the overall media disposal process of all paper assets within their scope.

The media disposal shall be commensurate with the data classification scheme. i.e. a document labelled Restricted, Confidential shall be disposed of in the manner required by the disposal of Restricted and confidential assets.

All paper assets shall be shredded using a paper shredder / incinerator.

In case of a copy machine jam or malfunction while a copy is in progress, the employee shall ensure that the paper is retrieved from the machine and disposed of in a secure manner.

5.4 Disposal of Electronic Media

The department heads shall be responsible for the overall media disposal process of all electronic assets within their scope.

The media disposal shall be commensurate with the data classification scheme. i.e. a document labelled as Confidential shall be disposed of in the manner required by the disposal of confidential assets.

Voice and video recordings shall be erased from storage media prior to their disposal. In case these recordings being on CD's, the CDs shall be broken / shredded.

External storage media like HDD's and USB Pen drives shall be formatted multiple times before disposal. A low-level formatting shall be done before reuse or disposal. A degaussing of the device shall be done before disposal of the same if necessary (Rev 2)

Sensitive data and licensed software shall be securely wiped off from all media before their disposal.

Media such as CDROM / DVD's etc., where it is not possible to wipe off the data shall be broken or shredded.

Before disposal of a PC / Laptop / smart phone / server, the data on is HDD, RAID array etc. shall be wiped off and then the asset disposed of.

5.5 Disposal of IT Assets

The IT team shall identify the obsolete IT assets in need of disposal. DO shall approve the same.

Asset disposal may take any form such as.

- Replacement with new assets under a buy-back option
- Selling the asset to the staff
- Donation to an organization / group
- Sale as scrap

Before the asset disposal, a backup of the data shall be done and handed over to the asset owner. The IT team shall ensure that all the data has been wiped off from the asset before its disposal.

The IT assets can be disposed of as and when the need arises. A review of the need for disposal shall be done on a yearly basis.

5.5.1 Disposal process outsourced

In case of the disposal process being outsourced

The external contractors responsible for the disposal should have proper security and process checks to ensure that information is disposed of in a secure manner.

Non-Disclosure Agreements shall be signed with the supplier prior to the start of the engagement. Confidentiality documents shall be signed with the vendor in case the media for disposal is being carried out of SISL's premises.

Certificates of secure disposal shall be obtained from the vendor.

The external contractor shall provide a list of personnel who will require access to the secured disposal area.

Disposal of confidential and internal data shall be logged.

5.5.2 Disposal of Non-IT assets

Non-IT assets (UPS, AC, etc.) but relevant to the information processing function shall be disposed of securely.

5.6 Incident Management

Any data breach due to a lapse in the asset disposal policy shall be considered as an incident and treated accordingly. This shall be in compliance with the Incident Management Policy.

5.7 Change Management

Any changes to the asset disposal process shall be in compliance with the change management policy of SISL.

6 Reference

Ref: - SISL-IT-PRO-Asset Disposal 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