SISL-IT-POL-Information Archival, Retrieval & Deletion Policy

Version No: V 1.0

INTERNAL DOCUMENT

OCTOBER 2025

Document Control

Document Name	SISL-IT-POL-Information Archival, Retrieval and Deletion Policy
Abstract	This document describes information archival, retrieval and deletion 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 is created and stored electronically as well as on hard copies. The data may be required at some later date and hence a need for data archival and easy retrieval.

An archive is a collection of computer files or hard copies of documents that have been packaged together for backup, to transport to some other location, for saving away from the computer or office location so that more hard disk storage or storage space can be made available, or for some other purpose. An archive can include a simple list of files or files organized under a directory or catalogue structure (depending on how a particular program supports archiving).

2 Policy Statement

Data archival and retention provides a systematic review of the retention of data as part of its business process. The policy identifies information that shall be retained, the retention and archival mechanism

3 Scope

The policy applies to all information generated at Share India Securities Limited (SISL). This policy is also designed to ensure compliance with applicable data privacy laws, including the Digital Personal Data Protection (DPDP) Act, 2023, particularly in the retention and disposal of personal data collected from individuals.

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.	Human Resource	Ensure that all the users and staff at SISL are aware of this policy.
4.	IT Team	Responsible to understand and adhere to this policy and archive data as required and as per this policy.
5.	All users	Shall understand and abide by this policy.

5 Definitions

5.1 Records

Records can be of any form either in electronic form or in paper document form which may contain data or information of any kind and in any form, created or received and accumulated by an organization or person in the transaction of business or the conduct of affairs.

5.2 Archive

Archives are those records that are appraised as having continuing value. The term Archive has been used here to describe records no longer required for current use which have been selected for defined period preservation for future reference.

6 Standards and Guidelines

SISL is committed to archive all its data as per the business requirement and to ensure availability, integrity and confidentiality of the said data.

6.1 Archival System

SISL shall build and manage an Archival System, to ensure that these archives are accessible by SISL as and when required.

6.1.1 Maintenance

The IT team shall be responsible for maintaining the online storage system.

6.1.2 Access to Archive

For efficient and secure operation of the Data Archival System, SISL shall store the data in a secure manner such that only authorized person has access to the same.

6.1.3 Security

In the process of archiving the data there shall be no loss of content. The archiving process shall not tamper the content of any data to ensure integrity of the data.

6.1.4 Encryption

SISL shall encrypt the data in the Data Archival System wherever possible so as to ensure confidentiality of the data.

6.2 Archival of hardcopies of documents / records

Hardcopies of documents and records for all specific projects shall be archived in file cabinets for the period defined as per business requirement. Access to the file cabinets shall be

available to authorized personnel only. The keys to these file cabinets shall be kept in the safe custody of authorized SISL personnel only. All the accesses to the keys shall be recorded.

6.3 Authorization

The request for archival or retrieval of specific data shall be duly authorized by the department head.

6.4 Retention

SISL shall retain the data for the period defined by the information owner. When the retention period of the data expires, with due consent from the concerned information owner, SISL shall erase or destroy the data in a manner adequate with its technology and as agreed with the information owner.

The disposal of the data shall be authorized by the department head.

All data related to statutory requirements shall be retained till the time frame defined. The data shall then be declassified and destroyed.

6.4.1 Records Maintenance

- Records shall be established and maintained to provide evidence of conformity to requirements and effective business operations.
- Records shall comply with legal and regulatory requirements, applicable standards and SISL's policy and contractual agreements.
- Records shall remain readily identifiable and retrievable.
- All records shall have identifiable information by which it can be identified based on requirement.
- Record backup shall be in compliance with the Backup and Restoration policy.

6.4.2 Record Security

All records shall be maintained in a safe and secure environment and protected from unauthorized users.

6.4.3 Record Retention

The retention period indicates the minimum time period for which the record shall be maintained.

The retention period shall be determined based on

- The business requirement
- Legal and Regulatory compliance
- Contractual obligations

In case the record is required even after the retention period is over, the record owner shall inform the IT team and the record shall be protected appropriately.

The below table outlines the retention period of various kind of records

Record	Recommended Retention Period	Deletion Method
Master Database (managed Service) (client ID, name, etc.)	Perpetual	Not to be deleted
Transactional Data – Definition (managed Service/trading information)	180 days or till the time the 1Tb HDD is full	Share this data with the managed services client in a secure manned after which the data on HDD is purged and a fresh back up is resumed.
Transactional Logs (Managed Services)	180 days or till the time the 1Tb HDD is full	Share this data with the managed services client in a secure manned after which the data on HDD is purged and a fresh back up is resumed.
Transactional Logs (Deployed Customers)	Managed and maintained by the customers. SISL does not maintain any logs.	Not Applicable, deleted by the customer as per their internal policy.
Email	5 Yrs	Deletion / Archive
Audit Trails (General)	1 Yr	Overwritten
Error Logs	180 Days	Overwritten
HR's employee records	1 Yr after the employee resigns	Shredding / Deletion
Financial Records	7 yrs /or as per legal requirement.	Shredding / Deletion
Legal Documents	Permanent	NA
Contract documents	1Yr after the contract expires / or as per legal requirement.	Shredding / Deletion

6.5 Disposal

The data disposal shall be in complaint with the Asset Disposal Policy.

6.6 Information Deletion

Information stored in information systems, devices or in any other storage media shall be deleted when no longer required to prevent unnecessary exposure of sensitive information and to comply with legal, statutory, regulatory and contractual requirements for information deletion.

6.6.1 Guidelines

Sensitive information shall not be kept for longer than required to reduce the risk of undesirable disclosure. When deleting information on systems, applications and services, SISL shall consider the following:

- Selecting a deletion method (e.g. electronic overwriting or cryptographic erasure) in accordance with the business requirements and taking into consideration relevant laws and regulations.
- Records shall be preserved for deletion as evidence.
- Evidence shall also be preserved when using services provided by external suppliers of information deletion.

Where third parties store SISL's information on its behalf, SISL shall consider the inclusion of requirements on information deletion into the third-party agreements to enforce it during and upon termination of such services.

6.6.2 Deletion Methods

SISL shall consider relevant legislation and regulations, sensitive information shall be deleted when no longer required, by:

- Configuring systems to securely destroy information when no longer required (e.g. after a defined period subject to the topic-specific policy on data retention or by subject access request);
- Deleting obsolete versions, copies and temporary files wherever they are located.
- Using approved, secure deletion software to permanently delete information to help ensure information cannot be recovered by using specialist recovery or forensic tools.
- Using approved, certified providers of secure disposal services.
- Using disposal mechanisms appropriate for the type of storage media being disposed of (e.g. degaussing hard disk drives and other magnetic storage media).

Where cloud services are used, SISL shall verify if the deletion method provided by the cloud service provider is acceptable, and if it is the case, the organization shall use it, or request that the cloud service provider delete that information.

SISL shall try to automate these deletion processes in accordance with topic-specific policies, when available and applicable. Depending on the sensitivity of information deleted, logs can track or verify that these deletion processes have happened.

To avoid the unintentional exposure of sensitive information when equipment is being sent back to vendors, sensitive information Shall be protected by removing auxiliary storages (e.g. hard disk drives) and memory before equipment leaves the organization's premises. Considering that the secure deletion of some devices (e.g. smartphones) can only be achieved through destruction or using the functions embedded in these devices (e.g. "restore factory settings"), SISL shall choose the appropriate method according to the classification of information handled by such devices.

Control measures described in ISO 27001 clause 7.14 shall be applied to physically destroy the storage device and simultaneously delete the information it contains.

An official record of information deletion shall be preserved as it is useful when analyzing the cause of a possible information leakage event.

6.7 Exceptions

Exceptions to the above policy shall be documented, justified and approved by the DO

6.8 Change Management

Any changes to the data archival system or the infrastructure used for data archival shall follow the Change Management Policy.

6.9 Incident Management

All incidents related to disruption in services leading to the irretrievability of the information shall be considered as an incident and duly reported. This shall be in line with the incident management policy.

7 Reference

Ref: 1. SISL-IT-POL-Backup and Restoration Policy

2. SISL-IT-POL-Log Management and Monitoring Policy V

8 Policy Review Frequency

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

9 Policy Exception

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

10 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