Share India
You generate, we multiply

SISL-IT-POL-Backup and Restoration Policy

Version No: V 1.0

INTERNAL DOCUMENT

OCTOBER 2025

Document Control

Document Name	SISL-IT-POL-Backup and Restoration Policy
Abstract	This document describes backup and restoration 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

Backup of business-critical information shall be taken on a regular basis in Share India Securities Limited (SISL). Adequate and appropriate backup and recovery procedures shall be defined, documented and implemented to ensure that all the business-critical information and software can be recovered post disaster or failure of the media. This would help prevent data loss, which can adversely impact SISL in terms of delays, business cost, loss of credibility, business etc.

2 Policy Statement

SISL generates quantum of data during the course of its business activities. It is very important to safeguard this information so as to ensure that, in the event of a disaster this information can be restored with minimum loss.

Information system owners shall ensure that adequate backup is taken such that data is not lost in the event of a disaster and that the data can be recovered in case of an equipment failure, intentional or unintentional destruction of data or a disaster.

3 Scope

The policy applies to

- All critical IT assets of SISL
- All critical information stored on the SISL computing platforms.
- IT Team responsible for the management of these critical computing systems.
- Development team is responsible for the management of critical source code, application, environment configuration.

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 this policy.
3.	Concerned Department Heads	Identify Business sensitive data, related application systems and important folders to be backed up and ensure that the restored data is tested and signed off

4.	IT Team	Manage the backup and Restoration process end-to-end.
5.	Development Team	Manage critical source code on company's code repository and backup and restoration of application and application containers.

5 Standards and Guidelines

The IT Team shall have a documented procedure that addresses the backup and restoration process for

- Source Codes and test results
- Application executable
- Application data files
- End user documents
- Electronic mails
- System software like Operating system, VM server configurations, cluster configuration, load balancer configuration, etc.
- Network device configurations
- Database files

Backup and Recovery plans shall be developed and shall be retained as per data retention policy.

The backup policy shall be reviewed on a regular basis or whenever there is a change in the backup process.

In case of a backup failure, either due to software or due to the media, the ISM shall be notified, and appropriate action taken.

5.1 Information Identification

5.1.1 Backup

The application owners shall be responsible for the identification of critical business applications and associated data, files and folders to be backed-up. This information shall be provided to the IT Team.

The new application / data identified and classified as business critical with a need for backup shall be communicated to the IT Team by the respective user manager.

The application software source / executable shall be backed up whenever a change is carried out in the application, or the application is upgraded.

Data files of the application software shall be backed up in line with the application's recovery point objective. (refer BIA column RPO (Recovery point objective)

5.1.2 Restoration

Any users with a restoration request shall forward their request to their respective user manager. The user shall clearly specify the data to be restored and the reason for restoration. The IT Manager shall authorize the execution of the request.

5.1.3 Exclusion

Application / Information owners shall share information on all the data that need no longer be backed up or that should be excluded from the backup.

5.1.4 Request Format

The Backup and Restoration Request shall be logged on to the helpdesk tool for initiation of a backup or restore request.

5.2 Backup Schedule

The IT Team shall work with the information owners to draw up a backup schedule. The backup schedule shall cover.

- Type of backup – full, incremental etc.
- Media / storage on which to backup
- Frequency of the backup
- Time of the backup

5.3 Backup Media

Backup shall be done on suitable media or service as planned by the management.

5.3.1 Back-up media labeling

The backup media shall be properly labeled where required for identification and information classification. The label classification shall allow for the easy identification of the application and the backup dates.

e.g. \\Backup\Month\device\(identify with time stamp) - may be used

5.3.2 Backup media security

5.3.2.1 Logical Security

Backup media shall be secured against unauthorized access. The data in the backup media shall be encrypted or password protected so as to ensure that in case of media loss, the data cannot be compromised.

5.3.2.2 Physical Security

The backup media shall be secured against physical threats onsite, offsite and during transit.

5.3.2.3 On-site Storage

The backup media shall be stored safely and securely. Server room shall be access controlled.

5.3.2.4 Offsite storage

The IT Team shall maintain a log of backup transferred to remote sites and shall ensure security of the data transfer and stored. Primary and secondary contact personnel details at DR site shall be maintained by the IT Manager and made accessible to the IT Team.

The offsite backup shall be maintained at SISL's other office premises or professionally serviced DC/DR provisioning centers.

5.3.2.5 During transition

The backup media shall be protected to prevent damage and tampering while the media is in transit. The media movement shall be registered in a separate media movement register.

5.3.3 Environmental Security

The backup media shall be secured against environmental threats.

- Environmental conditions like dust, humidity, fire etc. shall be taken into consideration while selecting the storage for the media.
- Storage media shall not be exposed to sunlight or heat generating sources.

5.4 Backup Software security

The backup software shall be adequately protected through logical and physical access control.

The following shall be ensured:

- The application is hosted on a secured and hardened Operating system.
- Access to the software shall be restricted to authorized personnel only.
- The software is tested before deployment in the production environment.
- The backup software shall be tested for its proper functionality.
- The backup software shall be automated with very little or no human intervention.
- In case of a change in the backup media, all previously backed up data that is required to be retained shall be transferred to the new media.

5.5 Backup / Restoration Logs

The IT Team shall maintain details of all backup or restoration activities carried out by them. This information shall be logged into the backup register.

5.6 Restoration Testing

Restoration testing of the backups shall be performed. The IT Team shall ensure that restoration tests are conducted at least once every six months, in accordance with the defined schedule, and that all test activities are properly recorded in the backup register.

5.7 Data Retention

Data shall be retained for a period necessary to satisfy business, legislative and contractual requirements. The data owners shall identify the retention period for essential business data and establish requirements for archive copies to be retained.

5.8 Data Archival

The information owner shall define the duration for data retention. The data shall be archived after its retention period has elapsed. Inactive data not accessed frequently shall be archived and maintained at a safe location.

Prior to the data archival process, a risk assessment shall be done on the data and measures taken to mitigate these risks.

The data archival process shall be as per SISL's Data Archival and Retrieval Policy.

5.9 Incident Management

Any disruption to backup and restoration shall be logged as an incident and shall be in compliance with the Incident Management Policy.

5.10 Change Management

Any changes to the backup and restoration process shall be made as per the Change Management Policy.

6 Reference

Ref: SISL-IT-PRO- Backup and restoration 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