SISL-IT-POL-DLP and Malware Management Policy

Version No: V 1.0

INTERNAL DOCUMENT

OCTOBER 2025

Document Control

Document Name	SISL-IT-POL-DLP and Malware Management Policy
Abstract	This document describes DLP and Malware 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 4

2 Policy Statement 4

3 Scope 4

4 Roles and Responsibilities 4

5 Antivirus Policy 5

5.1 Antivirus Software Procurement 5

5.2 Antivirus Software Installation 5

5.3 Antivirus Software Configuration 5

5.4 Antivirus Software Updation 5

5.5 Virus Infection 6

5.6 Next Generation Antivirus 6

5.7 Antivirus Server Security 6

5.8 Antivirus Logging and Reporting 6

5.9 Antivirus Monitoring 7

5.10 Antivirus Backup and Recovery 7

6 DLP Data Leakage Prevention Policy 7

6.1 Guidance 7

7 Incident Reporting 8

8 Change Management 8

9 Supplier Management 9

10 Reference 9

11 Policy Review Frequency 9

12 Policy Exception 9

13 Policy Violation Reporting Matrix 9

1 Introduction

Malwares includes all and any programs (including macros and scripts) that are deliberately coded to cause an unexpected and unwanted event on a user's workstation. Malwares includes viruses, worms, logic bombs, Trojan horses, web bugs, spyware, etc in Share India Securities Limited (SISL)

2 Policy Statement

All the information processing equipment including servers, desktops, laptops, etc. shall be protected against malicious code through the deployment of an enterprise level antivirus solution. The solution shall ensure early detection, efficient containment, and eradication of malicious codes.

3 Scope

This policy applies to

- All employees and third-party personnel using SISL facilities.
- All servers, laptops, desktops owned or leased to SISL.
- All computing devices owned by third party and connected to the organisations network for business purpose.

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.	IT Team	AV installation, updation, management, review and report
	All users	Shall report the following to the system administrator - Any virus / suspected virus activity. Notify the system Administrator / ISM before plugging any external laptop into the network. Ensure that pen drives, external hard disks, CDs used shall be scanned for virus.

5 Antivirus Policy

5.1 Antivirus Software Procurement

The IT team shall identify suitable antivirus software to be deployed at an enterprise level. The licensing requirements shall be addressed appropriately.

5.2 Antivirus Software Installation

- It shall be ensured that anti-virus software is installed on all the servers, workstations, and laptops which is in use.
- Cloud based anti-virus server shall be maintained by the service provider, SISL shall ensure all updates on servers, workstations, and laptops with the latest virus definitions / application.
- It shall be ensured that a new server, workstation, or laptop is installed with the anti-virus software and the latest virus definition / Application updated before it is connected to the network.
- Third-party systems like laptops, handhelds etc, shall not be plugged into the LAN unless it is installed with industry standard anti-virus software and updated with latest virus definitions (not applicable for EDR / XDR).
- The IT team shall scan the third-party devices before connecting it to the local network.

5.3 Antivirus Software Configuration

Anti-Virus software shall be configured for the following –

- Conduct scans as automated by the programme.
- Scan shall cover the following
    - Computer memory, executable files (including macro files), compressed files and removable storage media
    - Incoming and outgoing traffic (including e-mail and downloads from the Internet) must also be scanned.
- Provide an alert when AV version needs update and when a virus is detected.
- Disinfect the infected files and if this fails, delete the infected file.
- The anti-virus software shall be password protected to ensure that unauthorized users cannot uninstall the anti-virus software or alter the configuration settings of the anti-virus agent.
- Antivirus agent shall be configured for real time scanning to ensure that all viruses are detected, and appropriate action taken before they get activated.

5.4 Antivirus Software Updation

The following shall be ensured

- All desktops, laptops, servers, mobile computing devices shall be configured to receive an update from the service provider.
- In case of a stand-alone system including laptops (system which is not connected to the network) the antivirus software shall be updated manually.
- Those systems, not connected to the network and hence cannot receive an update from the cloud antivirus server, IT team shall verify the reason if left unattended for more than 60 days.

5.5 Virus Infection

In case an infected system is not cleaned, or the infected file cannot be deleted, the system shall be immediately taken off the network and manually cleaned as per the guidelines provided by the anti-virus vendor.

5.6 Next Generation Antivirus

SISL shall install and maintain a next generation antivirus which shall use advanced technologies like artificial intelligence, machine learning, and behavioural analysis to detect and prevent threats on endpoints.

The next generation antivirus shall have the following capabilities:

- Cloud-Native Architecture: Provide real-time protection without the need for constant signature updates
- AI and Machine Learning: Detect both known and unknown threats, including fileless and zero-day attacks
- Behavioural Analysis: Monitors and analyses behaviours to identify malicious activities.
- Integrated Threat Intelligence: Offer insights into adversary tactics and techniques.

5.7 Antivirus Server Security

Antivirus server security shall be managed and maintained by the service provider. SISL shall enable MFA for security.

5.8 Antivirus Logging and Reporting

The AV Logs shall be in compliance with the Log Management Policy.

Logging shall be enabled and shall cover the following

- Systems infected by virus and the action taken.
- Systems status with regards to the virus definition updates.
- The configuration of virus protection software has not been altered.

The AV reports shall be generated on a monthly basis and shared with the DO.

5.9 Antivirus Monitoring

New vulnerabilities which have been published and the threats to the environment due to that shall be tracked and steps identified for the mitigation of the associated risks.

5.10 Antivirus Backup and Recovery

The antivirus being a service, will not be backed up by SISL, service provide will ensure backup.

6 DLP Data Leakage Prevention Policy

SISL shall ensure that data leakage prevention measures are applied to systems, networks and any other devices that process, store or transmit sensitive information to detect and prevent unauthorized disclosure and extraction of information by individuals or systems.

Data leakage prevention inherently involves monitoring personnel's communications and online activities, and by extension external party messages, which raises legal concerns that shall be considered prior to deploying data leakage prevention tools. There is a variety of legislation relating to privacy, data protection, employment, interception of data and telecommunications that is applicable to monitoring and data processing in the context of data leakage prevention.

Data leakage prevention tools are designed to identify data, monitor data usage and movement, and take actions to prevent data from leaking (e.g. alerting users to their risky behaviour and blocking the transfer of data to portable storage devices).

Data leakage prevention can also be supported by standard security controls, such as topic-specific policies on access control and secure document and or information management.

6.1 Guidance

SISL shall consider the following to reduce the risk of data leakage:

- Identifying and classifying information to protect against leakage (e.g. personal information PII etc);
- Monitoring channels of data leakage (e.g. email, file transfers, mobile devices and portable storage devices);
- Acting to prevent information from leaking. (e.g. in case DLP is implemented)

SISL shall ensure data leakage prevention tools shall be used to:

- Identify and monitor sensitive information at risk of unauthorized disclosure (e.g. in unstructured data on a user's system);
- Detect the disclosure of sensitive information (e.g. when information is uploaded to untrusted third-party cloud services or sent via email);
- Block user actions or network transmissions that expose sensitive information (e.g. preventing the copying of database entries into a spreadsheet).

- SISL shall determine if it is necessary to restrict a user's ability to copy and paste or upload data to services, devices and storage media outside of SISL. If that is the case, SISL shall implement technology such as data leakage prevention tools or the configuration of existing tools that allow users to view and manipulate data held remotely but prevent copy and paste outside of SISL's control.
- If data export is required, the data owner shall be allowed to approve the export and hold users accountable for their actions.
- Taking screenshots or photographs of the screen shall be addressed through terms and conditions of use or through training and/or auditing.
- Where data is backed up, care shall be taken to ensure sensitive information is protected using measures such as encryption, access control and physical protection of the storage media holding the backup.

Data leakage prevention shall also be considered to protect against the intelligence actions of an adversary from obtaining confidential or secret information (geopolitical, human, financial, commercial, scientific or any other) which can be of interest for espionage or can be critical for the community.

7 Incident Reporting

Response to an outbreak of virus infection shall be addressed as per the Incident Management Policy.

The user shall report an antivirus incident to the relevant team. The responsible team shall take immediate steps to limit the extent of the damage.

The following steps shall be taken for speedy recovery

- Inform the DO
- Contact the antivirus vendor for assistance in containing the spread of the virus.
- Inform the other application / process owners about the incident.
- Take necessary steps to clean the virus.
- Take adequate steps to monitor the network for any virus traces.

8 Change Management

All critical changes to the antivirus infrastructure shall be in compliance to SISL's Change Management Policy.

This shall include but not be limited to

- Operating system / Change in Antivirus solution
- Changes in the antivirus architecture or update schedule

9 Supplier Management

The service level agreement with the antivirus vendor shall include the following provision

- Provide signature updates / newer versions of the software
- Provide technical support including onsite support within a specified time period.
- Contact person and response times for technical escalations.

10 Reference

Ref: SISL-IT-PRO-DLP and Malware Management Procedure

11 Policy Review Frequency

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

12 Policy Exception

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

13 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