SISL-IT-POL-Email Security Policy

Version No: V 1.0

INTERNAL DOCUMENT

OCTOBER 2025

Document Control

Document Name	SISL-IT-POL-Email Security Policy
Abstract	This document describes Email Security 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

Electronic Mail or e-mail is a computer facility available throughout Share India Securities Limited (SISL). It is intended to promote effective communication within the organization as email has the advantage of being faster, cheaper and more reliable than paper-based mail systems.

It is fundamentally important that e-mail be treated like any other form of written communication. Employees should always bear in mind that it is not a private communication facility.

2 Policy Statement

This policy aims to provide guidance, together with formal statements concerning the position of SISL, in relation to the use of e-mail and other electronic messaging systems. It also aims to assist staff in understanding the role of e-mail and to exercise appropriate judgment in the use of this tool. This policy builds on and complements other policies and procedures, in particular those relating to the IT Security, Human Resources policies and procedures.

SISL acknowledges that e-mail abuse can have serious disadvantages. This policy therefore aims to guide employees on the use of e-mail for the primary purpose of effective communication within the workplace, set down standards in respect of acceptable behaviour and email usage and reinforces the employee's responsibility to act within these guidelines.

3 Scope

This policy is applicable to all users of SISL using the e-mail facilities

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 users and staff are aware of this policy and abide by it.
4.	Users / Contractors	Are responsible for adhering to the policy

5 Standards and Guidelines

All users and staff of SISL using the official e-mail represent the company. They shall ensure that e-mail communication is used in an effective, ethical and lawful manner.

The responsibilities of all staff at SISL include, but are not limited to –

- Ensure that all communications are for professional reasons, relating to SISL business and they do not interfere with the user's productivity.
- Being responsible for the content of all text, audio, or images that they place or send by e-mail. All communication shall bear clear reference to its source of origin.
- Know and abide by all applicable policies dealing with security and confidentiality of SISL's records.

In addition to the above responsibilities, and to ensure that all users and staff at SISL are responsible and productive e-mail users and to protect the company's interests, the following dos and don'ts have been established.

The IT Team shall ensure the following disclaimer message is appended with all the email messages that are sent out of SISL domain.

> Information disclaimer: IMPORTANT: The contents transmitted by way of this email and any attachments herein are confidential and intended only for the person to whom it is addressed. This email may contain proprietary, business-confidential, and/or privileged material. If you are not the intended recipient of this message, any use, review, retransmission, distribution, reproduction, or any action taken in reliance upon this email should not be done and is strictly prohibited. If you have received this email by mistake, please notify the sender immediately and delete this email and any attachments contained herein from all computers. Disclosing the contents of this email to anyone or making copies thereof, without prior consent of the sender, is strictly prohibited.

The IT Team shall ensure all external emails are identified at the header for the user to be cautious while handling out of domain emails.

[EXTERNAL EMAIL]
DO NOT CLICK links or attachments unless you recognize the sender and know the content is safe.

5.1 Acceptable Use

- Use e-mail for business communication.
- All information sent and received on your corporate mail-id shall be treated as confidential/ Internal.
- Always compress (zip/rar) bigger files that are attached to email messages.
- Always report and delete any spam mail received in the mailbox.
- For email access via the web browser, the save password option should not be selected.
- The mailbox size is restricted as per SISL policy.
- The total mail size is restricted as per SISL policy.
- Internal e-mails shall be concise and directed only to those individuals who need to receive the information.

- E-mails shall be labelled to enable readers to gauge their priority, and attachments shall be labelled in a clear form to enable readers to identify their contents without opening them.
- Employees shall be aware of the risk of delivery failure when using e-mail for time critical business. Where the e-mail system is used for time critical business, the employee shall check that the e-mail has been received, either by using the facility in the e-mail package or by telephoning the recipient.

5.2 Unacceptable Use

All users and staff at SISL shall not use their official e-mail for purposes that are unrelated to the company's business activities, illegal, unethical, harmful to the company, or nonproductive. The following rules shall be followed.

- Do not send / forward chain e-mail.
- Do not conduct any personal business using company e-mail.
- Do not transmit any content that is offensive, harassing, or fraudulent.
- Do not encourage attachments including, images, audio or video clips in the company mailbox unless it is related to business needs.
- Do not give corporate e-mail id on non-commercial web sites where registration is required. If registration is required, provide an alternate external e-mail address.
- Do not try to access another employee's mailbox. In case of an emergency, the IT team shall provide access to a user's mailbox after proper authorization has been obtained by the employee from his / her Department Head.
- Do not open e-mails and their attachments that arrive from unreliable / unknown sources.
- Do not auto forward your e-mails to any external mailbox without getting necessary approval from the Department Head.
- Do not use scanned hand rendered signatures in e-mails.
- Servers shall not be used for accessing e-mails.
- Employees shall not be permitted to use personal e-mail ID during office hours, as its usage affect normal network traffic or interfere with the employee's attention to their duties.
- Employees may only use Company e-mail ID during working hours & not for their own personal use at times outside of their normal contractual working hours (Note: that throughout this policy the meal break is the only break that is deemed as outside of normal working hours and therefore a legitimate time for personal use).
- SISL reserves the right to prohibit all use of e-mail for personal use. Any employee found abusing this facility or using it inappropriately, in any way, including to request, create or forward any material which is obscene, indecent, discriminatory (on grounds of sex, race, disability, sexual orientation, age, religion / beliefs and gender), defamatory, illegal, or contains sensitive political views. These activities could be about, or to any other person

or organization. E-mail shall not be used for the expression of ill-will or bias against individuals or groups and shall not contain foul or offensive language.

- Employees shall be aware that downloading or transmitting the works of other people without their permission may infringe the laws relating to copyright / Intellectual property. Clearly it depends on how information is obtained, from whom and in what circumstances as to whether there is a potential breach. Employees shall therefore seek advice from their superior if they are in any doubt in relation to this.
- Employees shall not download messages, attachments, or files onto their system without ensuring that they have been properly scanned for viruses.

5.3 Mail server controls

5.3.1 Email User ID

Creation of email users shall be done only after receiving an authorized request as per the Ticket raised by HR Dept in Helpdesk. Password rules as defined in the password management policy are also applicable here.

5.3.2 Virus and Spam protection

SISL shall implement suitable virus and spam control measures to minimize the chances of the spams infesting the user's mailbox or spreading unwanted messages from a user's mailbox.

5.3.3 Encryption

All POP3 and IMAP communication shall be encrypted for protection of sensitive information with approved and agreed means of encryption.

5.4 Reporting Harassment

Report the receipt of any offensive e-mails to the originator of the e-mails. However, if the sender does not stop sending such messages, report the incident to the IT head and the HR department.

5.5 Monitoring

All messages created, sent, or retrieved over the email are the property of the company and may be regarded as internal company information. SISL reserves the right to monitor the traffic being sent over its facilities for any inappropriate, abusive or unethical use of the facility. Employees who carry out any inappropriate, abusive, or unethical use of e-mail shall be held responsible and legal and / or punitive action shall be taken up against them. All communications, including text and images, shall be disclosed to law enforcement or other third parties without prior consent of the sender or the receiver.

SISL wishes to reassure its employees that it does not routinely monitor individual usage of the system. Furthermore, SISL will, when deciding whether individual monitoring is

appropriate, in any given circumstances, give full consideration to the rights of the employee and only proceed to monitor when this is deemed proportionate and reasonably necessary.

5.6 Security

Each employee given access to the e-mail system shall be responsible for ensuring that the computer terminals (and PC workstations) are not left open for use by unauthorized persons. Employees shall keep their passwords confidential and change it regularly. While leaving a terminal unattended or on leaving the office, the employee shall log-off from their mailboxes and shut down the system (or lock their workstation) to prevent unauthorized users using the terminal in their absence.

5.7 Legal Action against the Company

Messages sent via e-mail can give rise to legal action against SISL and / or an individual employee for inappropriate or misuse of the system, in the same way as handwritten or typewritten messages. Claims of defamation, breach of copyright, confidentiality or contract could arise. As such, due care and diligence shall be exercised when sending all such messages.

5.8 E-Mail Abuse

Infringement of any part of this policy can lead to the matter being considered a disciplinary matter and appropriate action shall be taken.

In such cases SISL reserves the right to suspend internet access, (including email) pending the outcome of the disciplinary investigation.

Where an employee is suspected of inappropriate use or abuse of email, SISL may suspend their e-mail access, pending the outcome of the disciplinary investigation.

Examples of offences which may be considered to be gross misconduct which may result in dismissal are:

- Sending abusive, rude, obscene, pornographic, illegal or defamatory messages or material
- Sending a message that could constitute bullying or harassment.
- Compiling or distributing chain letters either internally or externally
- Sending confidential information without authorization
- Misuse of e-mail or the computer system, which results in a claim being made against SISL.
- Unauthorized copying or modifying of copyright material.
- Excessive personal use of e-mail.

Employees shall note that this list is not exhaustive.

5.9 Change Management

All major changes to the email system shall be done after a Change Request has been raised. The changes shall be in compliance with SISL's Change Management Policy.

5.10 Incident Management

All incidents related to the emails shall be logged. Incidents shall be addressed and resolved in compliance with SISL's Incident Management policy.

6 Policy Review Frequency

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

7 Policy Exception

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

8 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