Share India
You generate, we multiply

SISL-IT-POL-Application Security Policy

Version No: V 1.0

INTERNAL DOCUMENT

OCTOBER 2025

Document Control

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

Application Management involves handling and management of application as it goes through the entire application life cycle. The life cycle encompasses both application development and application management activities.

Application Development: Concerned with activities needed to plan, design and build an application that ultimately is used to address a business requirement. This also includes application acquisition, purchase, hosting and provisioning

Application Maintenance / Management: Focuses on activities that are involved with the deployment, operation, support and optimization of the application.

IT systems existent in Share India Securities Limited (SISL) need to be securely protected using various security controls. Applications are vulnerable to various kinds of attack which if exploited by a malicious user could lead to scenarios wherein security controls like authentication mechanism can be easily bypassed.

2 Policy Statement

Applications deployed in SISL infrastructure shall have controls to secure the input, processing, storage and output of data. The application shall be tested for security and performance before deployment and shall be managed for high availability. The access to the application shall be restricted to authorized users and access provided on a need-to-know basis.

3 Scope

The policy covers all applications deployed within SISL.

4 Roles and Responsibilities

Sr. No.	Role	Responsibility
1.	Designated Officer (DO)	Enforce and ensure that this policy is effectively implemented.
2.	IT Team	Implement and adhere to the policy and abide by it.
3.	Development Team	Implement and adhere to the policy and abide by it.

5 Standards and Guidelines

5.1 Application Security Controls

5.1.1 Access Control

Access to SISL application resources shall be restricted to authorized users only. Assigning individual user rights shall protect application system resources. Application security is the responsibility of all users, and the IT team is just a facilitator in this process.

Access restrictions shall involve setting up formal procedures to grant access to various application menu options and privileges to users so as to modify the data or execute commands, transactions or programs and authorization of these access rights by functional heads and data owners. Users shall be given access rights commensurate with their job function and this shall be governed by the principle of least privileges and 'need to know' basis. All secure applications shall implement authorization of users in addition to authentication.

Access rights shall be granted as per the Logical Access Control Policy.

Application shall have authentication and authorization controls.

- Application shall authenticate the users before providing access.
- Application shall have the mechanism to allocate user rights on the least privilege principle.
- Role-based access control shall be defined.
- Application shall restrict menu options based on a need-to-know and need-to-do basis.
- Access shall be granted only after relevant approvals have been obtained.
- Application shall ensure that a maker-checker concept has been built into its logic.
- End users shall not be able to invoke OS level / database level calls through the application interface
- Application shall use secure channels of data transmission for sensitive information.
- Application shall be designed to generate logs.
- The application owner shall prepare an access control matrix to grant access and privileges to the application users.
  - Name of the application
  - Version number
  - User department
  - User type (level, designation in the department)
  - User job profile
  - Access rights in the application
- The access control matrix shall reflect the operating system and database level access granted to the application user and system administrator.
- Any changes to the access privileges shall be made after an approval has been obtained from the user manager. The manager shall forward this request to the DO for approval. The

approved request shall then be sent to the authorized personnel to make the necessary changes

- All these access change requests shall be logged in to the helpdesk software.
- The application shall be hosted behind a firewall and access to the application shall be controlled.

5.1.2 Passwords

Application user-id and password features shall be used whenever available. Following password procedures shall be enforced for all application systems:

These shall be implemented in line with 'password policy'.

5.1.3 Data Security

- Sensitive data shall be stored in a secure manner.
- Application shall have the facility to check the integrity of the data.
- All data handled by the application shall be retained as per SISL data archival and retention policy.
- Application server shall be secured

5.1.4 Segregation of duties

To ensure a good internal control system as well as to minimize the risk of negligent or deliberate system misuse, the management and execution of business duties shall be separated. It is the responsibility of application and functional heads to ensure adequate segregation of duties. Critical areas where segregation of duties is required to be placed include update of master files and parameter files, system administration, security audit and systems development and maintenance.

5.1.5 Control of Operational Software

Implementation of software on the production systems shall be well controlled. All software's shall be tested in the test environment. These shall be deployed on the production servers after successful testing and sign off.

It shall be ensured that application program files have appropriate access controls. Moreover, the source code of the applications shall not be loaded on live systems. Only the required object codes and run-time versions shall be installed on the live systems.

Previous versions of the software shall be retained as a contingency measure. Suppliers provided software shall be maintained at a level supported by the supplier.

Software Patches shall be applied regularly to fix various bugs and defects.

5.1.6 Log Management

5.1.6.1 Secure Logging Practices

Adhere to logging standards and secure logging practices. Writing sensitive information (e.g. user passwords, database connection details including passwords) into log files could lead to compromising security. Additionally, it is important for logs to be standardized for easy accessibility and analysis.

The application shall be designed to log the following details

- User Account Management
- User Privilege Changes
- User Login / logout time
- Application configuration change
- Authentication failures

5.1.6.2 Error Logs

The application shall be designed to capture events and generate event messages.

The following shall be ensured

- The error messages shall not disclose critical information.
- The error shall not reveal information to the end user about the correct input required.
- The error message shall not reveal information about the application and the database.
- Custom error messages shall be used by modifying the default error messages.

5.1.6.3 Audit trails and exception reports

Audit trail shall be enabled in the application. Audit logs shall be generated for modification of master file records, key transaction entries; exception reports shall be generated using reports in application system or through backend such as: structured query language (SQL) or by way of report writer utilities.

These audit trials shall be made available and reviewed on a periodic basis. Furthermore, the audit logs shall be retained for a duration specified in the data archival and retention policy.

Following particulars shall be captured in the audit trails:

- Changes to parameter files, master files and static data
- Complete history of changes including old data, new data, user-ID, time, date etc.
- Main data filtering conditions and report criteria.

DO shall be responsible for the identification of the audit trails and exception reports required depending upon clear business process control objectives. Once the business requirements are clear, the IT team shall develop these audit trails and exception reports using appropriate system tools such as SQL, report writers or new programs.

5.2 Change Management

Changes to application shall be controlled by the use of formal change control procedures.

All changes to the applications in the production environment shall be made as per SISL Change Management Policy.

5.3 Incident Management

All incidents covering application security breach shall be logged and governed by SISL Incident Management Policy

6 Reference

Ref: SISL-IT-PRO -Application Development and Maintenance 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