SISL-IT-POL-User Management and Access Control Policy

Version No: V 1.0

INTERNAL DOCUMENT

OCTOBER 2025

Document Control

Document Name	SISL-IT-POL-User Management and Access Control Policy
Abstract	This document describes user and access control 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

Access control is a mechanism to ensure that authorized personnel have access to the information and information processing resources that are assigned to them.

Logical access control ensures that only authorized personnel have access to the information or data in electronic form; this includes access to the Operating system, application and associated information in Share India Securities Limited (SISL)

2 Policy Statement

Access rights shall be given on the principle of least privileges. Access Control specifies who and which process has access to a specific system resource and the type of access permitted. Access Control protects business and mission critical systems from unauthorized access, fraud and abuse.

3 Scope

This policy applies to

- All computing infrastructure deployed in SISL.
- All applications used by SISL.
- All laptops & desktops used by the employees of SISL.
- All suppliers who work with SISL and have remote access to the SISL computing environment.

4 Roles and Responsibilities

Sr. No.	Role	Responsibility
1.	Designated Officer (DO)	Ensure that this policy is effectively implemented.
2.	Information Security Manager (ISM/IGM)	Enforce the policy.
3.	Concerned Department Heads	Identify access rights to be granted to the users.
4.	Human Resource	Ensure that all users are aware of this policy
5.	IT Team	• Creation / Deletion of User IDs. • Grant / Revoke access rights • Review and report

5 Standards and Guidelines

5.1 User Management

5.1.1 User Creation

A unique User ID shall be created for every individual to access the information processing facilities at SISL. IT department shall create a new user-id and provide the rights as requested by the user's department head or on request from HR department.

The User ID shall follow a standard naming convention and cover all employees, consultants, suppliers and contractors.

5.1.2 User rights modification

The HR department or the concerned business team head shall notify the IT department about modification of the rights of any user whose job functions have changed.

5.1.3 User Deletion

The HR department shall immediately notify the IT Department to disable / delete the user-id of any user who has resigned / are on sabbatical / has been suspended or terminated / absconding from the services of SISL. The HR department shall also mention the date on which the user id shall be disabled / deleted with the request. In emergencies, such requests can be made over phone; however, it shall be followed by an email.

On receipt of notification from the HR department, the IT Department shall immediately carry out the requested action on the specified date. All user-ids of ex-employees, that were disabled, shall be deleted after 15 days, this will provide sufficient time window for administrator to maintain the audit and system logs of the user as per log management policy, unless explicitly requested by the HR department or the business head or required as per Application dependency.

5.1.4 Deactivation of user-ids

A user-id shall be disabled, if a user has not logged in for more than 30 days, post approval has been from the user's manager. In case the owner of this user-id is no longer in the employment of SISL, the IT Team shall delete / deactivate the user id after the Department Head (Users IDs may not be deleted due to application dependencies, in that case these userIDs shall be deactivated). IT department shall periodically identify and disable redundant user IDs, ensuring that redundant user IDs are not issued to other users

Guest accounts shall be disabled on all systems.

5.1.5 Reactivation of User Accounts

The IT Team shall reactivate locked / disabled user accounts.

The user's immediate senior shall authorize the reactivation of the user account by communicating the same to the IT team or logging a request in the helpdesk tool.

5.2 System profiles

Prior to the creation of system profiles, the roles of typical business users with appropriate access shall be identified. Systems profiles with requisite permissions shall be created at the pre-deployment stage of the new application.

The system profiles shall take into consideration

- The access usage
- Segregation of roles
- Requirement for a maker-checker concept in the application
- Application's ability to apply granular access rights

The application owner shall initiate the process and finalise the system privileges for each profile in consultation with the business owner.

The access rights and the privileges shall be documented and maintained in a updated state.

Appropriate alternative mechanism shall be identified for those applications that do not support granular access privileges.

5.3 Access Management

Access rights shall be defined based on need-to-know, need-to-do, segregation of duties and individual accountability principles.

Access to specific functions within an information system and the level of access required shall be identified and documented. The access requirement shall be identified in coordination with the business owner.

Access to the systems shall be through a unique user ID and password. The user would be responsible for the security of their user ID and be accountable for all its action.

Access to critical systems shall be restricted by the implementation of a firewall.

Access to data on the local systems, server, storage system, networking devices, etc shall be controlled.

5.3.1 Shared user-IDs

Users shall not share their user-ids. If there is a business requirement or need to share user-ids, this shall be authorized by the DO. Details of such User IDs if created shall be shared solely within the designated members of the group.

5.3.2 Administrator (privileged) rights

Administrator logins and privileged access rights allow users to override system controls. Users shall not be allowed to work with “administrator” ID or with privileged rights. Where users need administrative rights for the execution of their job responsibilities, the IT Team shall provide the user with the privileged rights only for the required period. The Information Security Manager shall authorize such requirements.

Password of privilege IDs shall be stored securely in the DO’s custody.

5.3.3 Access Control List (ACL)

The IT Team shall maintain an access control list with details of the access given to a user.

The ACL shall be reviewed on a quarterly basis and shall be updated as and when any user Ids are created, modified, disabled or deleted from the domain.

5.3.4 Access for printing facilities

SISL shall ensure that access to printing facilities is provided to users on a need-to-do basis. Users, whose job description does not require printing, shall not be given access to printers.

It is the responsibility of users to ensure that printers are used for official purpose only.

Where applicable, senior personnel or departments processing sensitive information shall be provided with separate printer.

5.3.4 Network Access for supplier laptops

Supplier / Client’s Laptops shall not be allowed to connect to the SISL network. If any such laptop needs to be connected to the network, request/ ticket shall be raised for concern HOD, it will be approved by IT and guest login shall be given with limited access.

IT shall ensure that the supplier / Client Laptops are free from virus before allowing them to be connected to the Network.

5.3.6 Access to Storage media

5.3.6.1 Access to USB ports

To ensure that no unauthorized transfer of information takes place using the USB port, SISL shall disable the USB port on all the computing devices.

Any user who requires access to USB ports shall obtain an approval from their department head and the ISM. The Information Security Manager shall notify the IT department to provide the necessary access.

The IT department shall maintain a list of users who have access to the USB ports.

5.3.7 Email and Internet Access

Internet and email are provided to the employees to carry out business functions. Users shall comply to the Email policy and the Internet Access Policy.

5.3.8 Unattended systems

Unattended systems shall be logged-off or locked so that no unauthorized person can gain access to the same. If system limitations prevent locking of a workstation / server, suitable password enabled screen saver shall be used.

5.3.9 Desktop / Laptop systems

The access to the system folders or disk drives on individual PC's or laptops shall not be shared unless share level access controls have been enabled on the folder or the disk drive. All laptops / desktops containing critical data shall not have any shared folders.

Necessary precautions shall be taken by the laptop users to ensure the privacy and confidentiality of their laptop data.

Storage of high-risk data on laptop and desktop shall be minimized and protected through access control, encryption and data recovery plans.

5.4 Access right modification

All changes to access rights shall be logged in the helpdesk tool and approved by the respective business head / application owner.

Access rights shall be modified when the employee moves to another department / process.

5.5 Access right revocation

For users leaving the organization, access should be removed on the employee's last working day.

In case, the access is no longer required, the department head / application owner shall inform the IT team for access revocation. A request for the same shall be logged in the helpdesk software.

5.6 Access Right review

The access rights shall be reviewed by the Information Security Manager on a quarterly basis.

5.7 Logon Procedures

The logon procedures to computer systems shall be designed to minimize the opportunity of unauthorized access.

- The logon procedure shall not provide any information that may aid an unauthorized user to successfully logon to the system.

- Logon data shall be validated only after it has been entered.
- Logon process shall not reveal which part of the logon data is valid or invalid.
- The number of unsuccessful logon attempts shall be restricted to 5.
- The logon process shall record unsuccessful login attempts
- A time delay shall be enforced before allowing any further logon attempts.

5.8 Emergency Procedures

Emergency IDs with privilege access shall be used in the event of an emergency only.

Passwords of emergency IDs shall be stored safely in the DO's custody.

Only authorized employees shall have access to this ID in case of an emergency where the IT Team / IT head are not available / cannot be reached during an emergency

Whenever the emergency IDs are used, a log shall be maintained

All emergency actions that bypass normal access control procedures shall be logged and reported for immediate review to the designated authority.

5.9 Incident Management

Any incidents related to unauthorized access shall be logged as an incident and shall comply to the incident management policy.

5.10 Change Management

Any changes to the access management process shall be done through the change management process and shall be in compliance with the change management policy.

6 Reference

Ref: SISL-IT-PRO-Logical Access Control 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