SISL-IT-POL-Password Management Policy

Version No: V 1.0

INTERNAL DOCUMENT

OCTOBER 2025

Document Control

Document Name	SISL-IT-POL-Password Policy
Abstract	This document describes Password Policy 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

The first line of defence while accessing any system is usually a user identification code i.e. a username and an authentication mechanism. Passwords are a way of identifying a user based on the credential provided. They form a common means of validating a user's identity to access an information system or service. Improper management and use of passwords can result in security breach.

2 Policy Statement

Access to any information within Share India Securities Limited (SISL) shall be authenticated with a password or an access code. Management of these passwords or access codes is mandatory to maintain control over the use of systems, devices and the access to these protected resources.

3 Scope

The policy addresses effective password management.

The scope of this policy includes all personnel who have or are responsible for an account on any system that resides in has access to the SISL's network or stores any non-public data.

4 Roles and Responsibilities

Sr. No.	Role	Responsibility
1.	Designated Officer (DO)	Ensure that this policy is implemented effectively
2.	IT Team	Apply password settings as per the policy. Comply to the password guidelines for network devices, databases and applications
3.	Human Resource	Ensure that all users and staff read and abide by this policy
4.	Users	Shall be aware of the policy and follow the password guidelines.

5 Standards and Guidelines

5.1 Password settings

5.1.1 Password Length

Passwords used shall be 12 characters in length shall be used at a minimum as per regulatory directives.

5.1.2 Password Complexity

The combination of characters used shall be a mix of alphabets, numbers and special characters. Users shall not choose passwords which can be easily guessed, like names or part of names, dictionary words, phone numbers, dates or common words.

5.1.3 Password History

Password history shall be set to 5 This will prevent the re-use of the last 5 passwords.

5.1.4 Password Age

Password age shall be set to 45 days. A reminder shall be given to the user, 10 days prior to the expiry of the passwords. Failure to change the passwords before expiry shall result in the account getting locked / disabled.

5.1.5 Account Lockout

Where possible, systems shall be configured to lock the user's account if there have been more than 5 invalid login attempts. Reactivation of locked user accounts shall be activated within 15 minutes from receiving the request. Application shall logout the user session after -30 minutes of inactivity and redirect user to login page.

5.1.6 Password Change Alert

- 10 days prior to the expiry of the password, the user shall be alerted with a warning message at every login.
- System and Application shall verify the user's old password before it allows the user to change the password. "Remember Password" feature shall not be used in SISL applications.
- Passwords shall not be logged or captured in any logs management system.

5.1.7 Password Encryption

Passwords shall be encrypted when transmitted over the LAN, WAN and Internet.

The password display shall be masked so that the password cannot be seen by unauthorized users.

5.2 Password Management

5.2.1 Privilege ID Management

- All administrator passwords shall be kept in a secured location under the custody of the DO. In case of an emergency where password access is required the user will contact the DO for the same.
- For users who require administrative privileges to carry out their job functions, necessary privileges shall be granted to their user-id after appropriate approval is obtained from their department / process head and ISM
- The administrator passwords shall follow the same password settings as in point 6.1 above.
- In case an employee with administrative access to the systems part ways with the organization, the password shall be changed immediately.
- It is the user's responsibility to ensure that they maintain password confidentiality and acknowledge liability for transactions done using their ID's.

5.2.2 Default Password

The operating system and application vendors provide default user-ids and passwords. Where feasible, the default IDs shall be disabled. Where it is not possible to disable the ID's, default password set by the manufacturer of the product shall be changed prior to the introduction of the system / application in the production network.

5.2.3 One time Password

A temporary password shall be assigned or initial password when creating a new user account. The password shall be communicated to the user through SMS.

Users shall change their passwords after first successful login attempt. Where possible, systems shall be configured to force a user to change their initial passwords when they log on for the first time.

5.2.4 Multi-Factor Authentication (MFA)

All the systems should be configured to integrate Multi-Factor Authentication (MFA) to enhance security.

5.2.5 Password Reset

Temporary unique passwords shall be assigned to users when they request for password changes. Users shall be forced to change their password after their password has been reset.

The password shall be communicated to the user in a secure manner. Username and password shall not be sent on the same message.

5.2.6 Passwords of Network Device

Passwords of firewalls shall be changed as per active directory (AD), switches and wireless access devices shall be changed regularly. The password for these devices shall be with the concern member of IT infrastructure team and they shall ensure the security of the same.

5.2.7 Automated Log-on

Use of passwords in automated logon processes shall be avoided. Passwords shall not be included in automated logon processes; batch processes or hard coded in applications unless there is a business need for the same. For such exclusions, authorization of the Information Security Officer shall be taken.

5.2.8 Application Development

The application development team shall ensure that their program contain the following security precautions

- Application shall support authentication of individual users and not groups.
- Application shall not store the password in clear text or in any easily reversible form for critical applications.
- The application shall be designed to meet the password security requirements defined in 6.1 above.
- Application shall provide for role management so that a user can take over the function of the other without the need to share the passwords.

5.2.9 Customer facing passwords

Customer facing applications shall also follow the same password security criteria defined in 5.1 above or

The following pointers are applicable for clients only

a. Forgot password

b. Self-change password

c. Force-change expired password

d. Unlock account and change password

e. First time login using system generated password

5.3 Password Compliance

All ID's / applications / servers / network devices for which the password cannot be configured as per this password policy shall be documented and be available with the DO. Appropriate justification shall be provided for the same.

Disciplinary action shall be taken against users who violate the password 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