SISL-IT-POL-Change Management Policy

Version No: V 1.0

INTERNAL DOCUMENT

OCTOBER 2025

Document Control

Document Name	SISL-IT-POL-Change Management Policy
Abstract	This document describes Change 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

Unauthorized changes and unstructured implementation of information assets may lead to system downtime and unauthorized access leading to a breach of security.
All changes, irrespective of a major or minor change, shall be carried out after a proper analysis has been done, impact of change calculated, rollback (remediation) options worked out and a proper approval obtained.

2 Policy Statement

To ensure that all changes are reviewed, approved, scheduled, communicated, and implemented in a standardized manner that minimizes the impact of change related incidents and consequently improves operations for Share India Securities Limited (SISL).

3 Scope

The policy applies to

- All critical assets
- All persons responsible for implementing the changes.
- All persons responsible for change approvals
- All business or application owners responsible for the smooth functioning of the assets.
- Employee
- Contractors / Suppliers

4 Roles and Responsibilities

Sr. No.	Role	Responsibility
1.	Change Advisory Board (CAB)	Responsible for reviewing and approving or rejecting any changes.
2.	Change Manager	Overseeing the entire change management process
3.	Change Requestor	Initiator of any change
4.	Technical Staff	Responsible for implementing change

5 Standards and Guidelines

All changes initiated within SISL shall follow a proper change management process.

A change shall be defined as any addition, modification or removal of existing information processing system, information assets or supporting systems.

5.1 Change Management Cycle

CAB is designated as approvers and reviewers, responsible for approving and tracking critical changes. The approver and reviewer shall comprise of members from consolidated groups consisting of the following:

- Business team – Approver and Reviewer
- IT Infrastructure team – Approver and Reviewer
- Admin and Human Resource – Approver and Reviewer
- Operations team – Approver and Reviewer
- DO – Security incidents and changes related to information security.

5.1.1 Change Request

A formal change request shall be created by the change requestor who initiates a change. A change request shall be an individual request or an outcome of helpdesk / incident / Disaster Recovery process.

All changes shall be initiated by logging them into the Change Management Portal or via email. The Change Request shall capture the following information.

- Change owner details – Change initiator details shall be captured.
- Description of the change – The description shall cover details regarding configuration changes, installation of additional components and system restart requirements.
- Reason for the Change – A clear justification for a change which could include new business requirements, product features enhancements and problem rectification.
- Affected Users / Process / IT assets – List of users and departments impacted due to the change.
- Rollback plan – Any remediation plan or solutions which shall achieve the same objective / benefit without compromising security shall be documented.
- Change Authorization and approval – The change request shall be reviewed, authorized and approved by change approver before the change is initiated.

5.1.2 Change Analysis and Authorization

All change requests shall be classified into one of the below mentioned change categories:

- **Normal Change** - Any temporary or permanent change, with a certain level of risk, to an information processing system or the supporting services.

- **Standard Change** - A well-defined, fully documented change with very low or no risk.
- **Emergency Change** - A change required to a managed IT & non-IT environment because of sudden loss of service or disruption.
- **Major Change** – Multiple impact levels including regulatory etc.

5.1.3 Change Management Committee

The CAB shall conduct a feasibility study of the change and record the same in the change request form on the portal. Feasibility analysis shall cover the following.

- **Need for a Change** – The objective of the change shall be evaluated to ensure that it is in accordance with the business requirement.
- **Impact of the change** – The request for change shall be approved based on the business requirement, process improvement or security enhancement of the environment. The approval shall be recorded in the change management portal. The approver and reviewer shall ensure that the required controls for controlling any adverse impact on the systems and the time needed to implement the controls.
- **Change Criticality / Priority** – The criticality of the changes shall be evaluated, the priority defined for immediate changes or changes to be implemented at a later date and time.

Appropriate approvals shall be taken for the change depending on the impact, priority and size of the change.

5.1.4 Change Implementation Plan

After a change has been approved, an implementation team shall prepare a detailed implementation plan covering the following aspects of the change.

- Pre-requisites – Wherever the change requires a pre-requisite such as data backup prior to the change implementation, these shall be documented.
- Change window – The plan shall cover the downtime requirements and wherever possible, these shall be during non-peak hours.
- Implementation Steps – The implementation steps and the relevant people required for the implementation shall be documented in detail.
- Test Plan – The procedure for the testing of the changes and the people involved in the test shall be documented in a test plan.
- Remediation plan – The implementation plan shall also document the remediation plan so as to restore the system to its original state in case a successful change fails. The time and reason or the remediation shall also be documented.

The business / application owner shall inform the users and the implementation team about the changes to be implemented.

5.1.5 Change Testing

The changes shall be tested in a test environment, wherever applicable / possible, prior to making changes to the production environment.

- The implementation teams shall make the changes in the test environment as per the implementation plan and confirm the functionality of the system / process.
- Any deviation from the implementation plan shall be recorded and approved by the CAB.
- The teams responsible for the implementation shall test the roll back (Remediation) plan in the test environment.
- After successful testing, the CAB shall approve the implementation of the change to the production environment.
- Testing shall be done only where the Change Criticality / Priority is set as 4 or 5.

5.1.6 Change Implementation

The implementation team shall implement the changes to the production system in accordance with the implementation plan.

Segregation of duties shall be maintained during the implementation. Care shall be taken to ensure that the team that approves the change is not part of the implementation team.

A post-implementation report shall be prepared and submitted to the CAB. The report shall contain the details of the actual implementation encompassing.

- Implementation steps
- Test plan results.
- Deviation justification if any

The business / application owner shall ensure that the change authorized by the CAB has been implemented.

The change request shall be updated accordingly after a successful change implementation.

5.1.7 Change Monitoring and Verification

After the change has been successfully implemented, it shall be monitored for a few days to ensure that the change has not impacted on regular business operations.

The change shall be reviewed for effectiveness based on the following criteria.

- Change achieved the desired objective – CAB shall evaluate whether the objectives defined in the original change request have been met.
- Adherence to the implementation plan – the CAB shall evaluate whether the steps in the proposed implementation plan have been followed.

5.1.8 Change Remediation

The change shall be remediated if it is not applied successfully. An approval for the same shall be obtained from the CAB prior to the remediation.

After the remediation has been implemented, the system shall be verified by the business / application owner. They shall maintain records of the changes and the remediation activity.

5.2 Changes for Outsourced Services

Any changes to the IT processing systems hosted at another location other than the SISL premises and managed by the supplier shall be handled by the respective service providers and shall follow a proper change management process.

5.3 Emergency Changes

Emergency changes (system breakdown, priority system patch updates etc.) shall be carried out under exceptional conditions only. Such changes shall be carried out based on verbal approval from CAB.

It shall be ensured that integrity of the systems is maintained and there is no adverse impact on overall security during these emergencies. The following steps shall be adhered to in case changes need to be brought about in an emergency.

- Allow emergency fixes only to resolve production server problems.
- Return to normal change procedures expeditiously.
- All emergency changes shall be ratified by the normal change management process.
- Application and business owners shall document the changes and report the same to the CAB.
- The person / team of people responsible for implementing the change shall submit a post-implementation report to the CAB.
- All such emergency changes shall be approved, authorized and reviewed by the CAB.

5.4 Changes due to Incidents

All changes made to the production system due to an incident and subsequent changes to resolve the incident shall be accompanied by a corresponding incident management form / ticket.

5.5 Incident Management

Any change implementation that led to a disruption of services shall be treated as an incident and documented.

6 Reference

Ref: - SISL-IT-PRO-Change Management Procedure

SISL-IT-REC-Change Request Form

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