SISL-IT-POL-Configuration Management Policy

Version No: V 1.0

INTERNAL DOCUMENT

OCTOBER 2025

Document Control

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

Configuration Management is the discipline that identifies, records, controls and reports on the IT infrastructure components such as hardware, software, documentation, services, personnel and any other items (known as Configuration Items - “CI’s”) and verifies the completeness and correctness of the configuration items.

The main task of Configuration Management is to keep an up-to-date record of all the components in the IT infrastructure configuration and the interrelations between them.

Configurations, whether acting as a single config file, or a group of configurations linked together are the underlying parameters that govern how hardware, software and even entire networks are managed.

As an example, a firewall’s configuration file will hold the baseline attributes that the device uses to manage traffic to and from an organisation’s network, including block lists, port forwarding, virtual LANs and VPN information.

2 Definitions

- Configuration Items -
  - Hardware devices such as PCs, Laptops, Routers, Firewall, Manageable Switches, VM’s etc.
  - Software: Operating Systems, Applications, Network Protocols, etc.

    (Documentation: manuals, service level agreements, etc. related to configuration items)

- Configuration Management Database (CMDB) - This database includes:
  - Detailed information about each configuration item.
  - Interrelations between the different configuration items, such as "parent-child" relationships, or logical and physical interdependencies.

  The CMDB is not just a list of the stock or parts. It gives a global view of the organisation's IT structure.

3 Configuration Management Policy

3.1 Standard Templates

Standard templates for the secure configuration of hardware, software, services and networks shall be defined:

- Pre-defined templates from vendors and or from independent security organization shall be used using publicly available guidance. E.g. CIS benchmark (Centre for Internet Security) for Infrastructure, which provide guidance on how best to configure hardware and software assets.
- The templates shall be used considering the level of protection needed in order to determine a sufficient level of security, i.e. meet the minimum-security requirements for the devices, applications or systems that are applicable.
- The templates shall support SISL information security policy, topic-specific policies, standards and other security requirements, i.e. Work in harmony with SISL broader information security efforts, including all relevant ISO controls.
- The templates shall consider the feasibility and applicability of security configurations in SISL context. i.e. keeping in mind SISL unique business requirements especially where security configurations are concerned including how feasible it is to apply or manage a template at any given time.
- The templates shall be reviewed periodically and cater to system and/or hardware updates, or any prevailing updated when new threats or vulnerabilities need to be addressed, or when new software or hardware versions are introduced.
- Baseline configurations shall be formally defined, reviewed, and approved for all critical infrastructure components, including but not limited to firewalls, routers, database servers, core applications, and operating systems. These baselines shall serve as the minimum-security configuration standard and shall be reviewed at least quarterly or after any significant update or configuration change.

3.2 Configuration Security Controls

The following shall be considered for establishing standard templates for the secure configuration of hardware, software, services and networks:

- Minimizing the number of users with administrator privileges to a minimum.
- Disabling any unused or unnecessary identities.
- Disabling or restricting unnecessary functions and services.
- Restricting access to powerful utility programs and host parameter settings by closely monitoring access to maintenance programs, utility applications and internal settings.
- Ensure that clocks are synchronized in order to log configuration correctly and assist in any future investigations.
- Immediately changing any default passwords or default security settings that are supplied with any device, service or application and reviewing other important default security related parameters.
- Invoking time-out facilities that automatically log off computing devices after a predetermined period of inactivity.

- Implementing a default logoff period for any devices, systems or applications that have been left dormant or unlogged for a specified period of time.
- Verifying and ensuring that all licensing requirements have been met.

3.3 Managing configurations

Established configurations of hardware, software, services and networks shall be recorded and a log shall be maintained of all configuration changes. These records shall be securely stored. This can be achieved in various ways, such as configuration databases or configuration templates.

All changes to the configurations shall follow the change management process.

Configuration records can contain as relevant the following:

- Up-to-date owner or point of contact information for the asset.
- Date of the last change of configuration.
- Version of configuration template.
- Relation to configurations of other assets.

3.4 Monitoring configurations

Configurations shall be monitored with a comprehensive set of system management tools (e.g. maintenance utilities, remote support, enterprise management tools, backup and restore software) and shall be reviewed on a regular basis to verify configuration settings, evaluate password strengths and assess activities performed. Actual configurations can be compared with the defined target templates.

Any deviations shall be addressed, either by automatic enforcement of the defined target configuration or by manual analysis of the deviation followed by corrective actions.

SISL shall maintain and store configurations, including keeping an audit trail of any amendments or new installations, in line with a published change management process.

Logs shall contain information that outlines:

- Who owns the asset.
- A timestamp for the latest configuration change.
- The current version of the configuration template.
- Any relevant information that explains the assets relationship with configurations held on other devices or systems.

SISL shall explore to deploy a wide range of techniques to monitor the operation of configuration files across SISL network, including:

- Automation.
- Specialized configuration maintenance programs.

- Remote support tools that auto populate configuration information on a device-by-device basis.
- Enterprise device and software management utilities that are designed to monitor large amounts of configuration data at once.
- BUDR (Backup and Disaster Recovery) software that automatically backs up configurations to a secure location and restores templates either remotely or onsite to compromised and/or malfunctioning devices.

SISL shall explore possibility of implementing configuration specialized software to track any changes in a device's configuration, and take appropriate action to address the amendment as soon as possible, either by validating the change or reverting the configuration back to its original state.

4 Policy Review Frequency

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

5 Policy Exception

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

6 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