SISL-IT-POL-Capacity Management Policy

Version No: V 1.0

INTERNAL DOCUMENT

OCTOBER 2025

Document Control

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

Capacity Management is responsible for ensuring that all IT processing and non-IT support systems are well-supported by adequate and properly dimensioned capacity in Share India Securities Limited (SISL).

Without proper Capacity Management, resources are not utilized optimally, resulting in unnecessary investments leading to additional maintenance and administration costs or worse, insufficient resources being available, leading to degradation in quality of service.

2 Policy Statement

Capacity Management shall:

- Stay up to date with the current state of the technology and expected future developments.
- Know about the company's business plans and service level agreements in order to forecast the necessary capacity.
- Analyze the performance of the infrastructure in order to monitor the use of existing capacity.
- Design capacity models and run simulations for various possible future scenarios.
- Capacity to be identified for services and applications appropriately, aligning them with business processes and the customer's real needs.
- Manage demand for computing services by rationalizing their use.

3 Scope

This policy applies to all Assets of SISL

4 Roles and Responsibilities

Sr. No.	Role	Responsibility
1.	Designated Officer (DO)	Ensure that this policy is effectively implemented.
2.	Information Security Manager (ISM)	Enforce the policy.
3.	Asset Owner	Implement and Adhere to the policy.

5 Standards and Guidelines

The Capacity Management Policy shall address the capacity needs of the IT infrastructure from a security perspective.

5.1 Capacity Management Drivers

The capacity needs of the organization shall be determined based on the below factors.

5.1.1 Current Capacity

The current capacity of the system shall be analyzed to determine whether it meets the needs of the users.

5.1.2 Future Capacity Needs

By the use of forecasts for future business activity, future system requirements shall be determined. Implementing the required changes in system configuration shall ensure that sufficient capacity is available to maintain service levels, even as circumstances change in the future.

5.2 Capacity Planning Approach

This activity shall be broken down into

Data Gathering
Model Construction
Documentation of alternatives

5.2.1 Data Gathering

Types of measurement required are Hardware Usage, Workload and Program Measurement. It is at the discretion of the IT Manager to decide the extent and content of data that shall be captured based on the criticality of the server.

5.2.2 Model Construction

Taking into account the current and projected trends of information processing, new business and system requirements, future Capacity demands shall be computed by mapping the expected growth in business to ensure adequate processing power and storage. The forecasted capacity utilization shall take into account the desired service levels (e.g. response times, turnaround times etc.). Appropriate software and hardware tools shall be used to gather the data required. SISL shall use automated tools or other equivalent platforms for real-time and historical monitoring of system capacity, utilization trends, and threshold alerts.

5.2.3 Documentation of Alternatives

The trend analysis information related to hardware and application usage, which is collected, shall be presented to the IT Manager empowering him / her to identify and avoid potential bottlenecks that might present a threat to system security or user services, and plan appropriate remedial action.

5.3 Infrastructure Components Measurement

The Capacity Management shall cover the following Infrastructure components and within the infrastructure components the following shall be monitored:

5.3.1 Servers

Parameter	Escalation Trigger
CPU	80 % Utilization
Physical Memory	80 % Utilization
Used space	80 % Utilization
Uptime	99.99% Uptime

5.3.2 Storage Systems

Parameter	Escalation Trigger
CPU	80 % Utilization
Physical Memory	80 % Utilization
Used space	80 % Utilization
Uptime	99.99% Uptime

5.3.3 Switches:

Parameter	Escalation Trigger
CPU	80 % Utilization
Uptime	99.99% Uptime

5.3.4 Firewall:

Parameter	Escalation Trigger
Memory	80 % Utilization
Uptime	99.99% Uptime

5.3.5 Links:

Parameter	Escalation Trigger
Utilization	80 % Utilization
Uptime	99.99% Uptime

5.4 Capacity Measurement Records

Records of all monitoring activity shall be maintained. Trend Analysis of the same shall be done on a regular basis.

5.5 Capacity Reporting

Capacity Measurement reports of all devices within the gambit of this measurement shall be shared with the IT head.
Capacity Measurement reports shall also assist in the measurement of SLA's committed by the vendor and by SISL's IT team to its customers.
Capacity measurement reports shall be generated and reviewed on a monthly basis, and more frequently for high-risk or business-critical systems. These reports shall be retained for audit and trend analysis.

5.6 Incident Management

In case of an outage due to capacity-related issues, the same shall be logged in the Incident Report and a proper incident management process shall be followed in compliance with SISL's Incident Management Policy.

5.7 Change Management

Any changes to the IT infrastructure where the capacity of the existing systems is changed, the change management process shall be invoked and adhered to. The Change Management Process shall be in line with SISL's Change Management Policy.

6 Reference

Ref: SISL-IT-REC- Capacity planning

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