SISL-IT-POL-BCP & ITDR Policy

Version No: V 1.0

INTERNAL DOCUMENT

OCTOBER 2025

Document Control

Document Name	SISL-IT-POL-BCP & DR Policy
Abstract	This document describes business continuity and disaster recovery 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

Share India Securities Limited (SISL) recognizes the strategic, operational and financial risks associated with service interruptions and the importance of maintaining a disaster recovery plan that supports the continuation of services to the customers, clients and internal stakeholders.

IT disaster recovery programs are fundamental to ensure against organizational and reputation risks in the event of an extended business interruption or disaster.

SISL is committed to the establishment and maintenance of a comprehensive Information Technology Disaster Recovery program that will ensure the timely and effective recovery of its information technology assets that support the business function.

2 Policy Statement

SISL shall design and implement an IT DR management framework to improve its resiliency and ensure availability of IT systems supporting the business operations.

A formal governance structure shall be developed to ensure effective decision making and enabling timely recovery and restoration of IT systems.

An updated register of critical assets shall be maintained at all times.

A business impact analysis shall be carried out for all the functions to ensure that the organizational requirements are identified. The BIA shall document the dependencies on the underlying IT assets required for the functioning of the business process. The BIA shall determine the Recovery Time Objective (RTO) and the Recovery Point Objective (RPO) for each IT resource and application.

All IT assets shall be subjected to risk assessment on a periodic basis to identify the vulnerabilities that may have an impact on the IT assets availability.

Detailed Recovery procedures shall be documented for an effective recovery of the IT applications within the agreed upon recovery timelines.

SISL shall develop, exercise and maintain plans for the resumption and recovery of IT systems.

3 Scope

The policy applies to

- All Information technology assets are owned directly or indirectly by SISL.
- All employees, contractors and supplier staff who directly or indirectly are responsible for managing the information technology assets of SISL.

4 Roles and Responsibilities

Sr. No.	Role	Responsibility
1.	IT DR Steering Committee	• Oversight of IT DR governance process. • Ensure IT DR is in line with strategic and business objectives. • Review and approve IT DR Policy and framework. • Test IT DR Plans • Implement IT DR framework
2.	Designated Officer (DO)	• Ensure risk assessment is done for IT applications at least once in a year. • Ensure that all the statutory and regulatory requirements applicable to the ITDR program are met.
3.	IT Team	• Implement and abide by the policy. • Test the IT DR plans.
4.	Employees and Suppliers	• Abide by the policy

5 Standards and Guidelines

5.1 Business Impact Analysis

A business impact analysis shall be done for all the business-critical operations. Recovery Time Objective (RTO) and Recovery Point Objective (RPO) shall be defined for all the applications depending on business requirements.

All the dependencies on the IT systems by the business functions shall be clearly documented.

5.2 Risk Management and Evaluation

Adequate coverage shall be provided in the identification of threats that may cause disruption to the IT assets availability which supports business operations.

Each threat shall be assessed based on its impact and probability of occurrence. A risk rating shall be assigned.

A defined and documented risk assessment methodology shall be used for the risk assessment exercise. Risk Analysis shall be performed on a yearly basis. Risk Acceptance levels shall be defined, documented and approved by management.

Existing controls shall be assessed for their strengths and effectiveness. The mitigation of a risk due to the presence of existing controls shall factor in the control strength and its effectiveness value.

Control assessment shall be undertaken on a sampling basis and the sampling frequency shall be clearly defined.

A risk with ratings above the acceptable level of risk shall have risk mitigation plan defined and approved by the management. The risk mitigation plan shall clearly define ownership of the action items. Risk mitigation plans shall be reviewed and tracked to closure on a quarterly basis.

5.3 IT DR Strategies

IT DR strategies chosen shall be capable of supporting and integrating with the business continuity strategies of the organization.

Strategic options shall be evaluated for the technology components and appropriate strategies defined for recovery and restoration of IT systems based on their priority.

External products and services shall be covered by the strategic options chosen where appropriate.

5.4 IT DR Recovery Planning

The purpose and scope of the IT DR plan shall be defined, approved and understood. The plan shall set out prioritized objectives in terms of

1. Critical IT services to be recovered.
2. Time Span within which to recover.
3. Situation that invokes the plan.
4. Recovery level of each critical IT service.

The response and recovery plans shall be concise and accessible to those responsible for the same.

Stages of escalation and trigger events (interruptions, single point of failures) shall be clearly defined and used as a basis for the development of IT DR recovery procedures.

Specific IT DR Plans shall be documented and approved. IT DR shall provide detailed instructions on the recovery and restoration of IT processes and system.

1. Technology recovery procedures shall be developed and shall cover the following areas.
2. Detailed procedures to restore the application, database and associated hardware at an alternate location or local depending on the nature of disruption or disaster, taking into account the changed environment.
3. Detailed procedure to restore the network accessibility.

4. Procedures for data synchronization and handling of the backlog information resultant of the outage.
5. Changes required by the end users to access the application.

IT DR plans shall be reviewed on an annual basis.

5.5 Training and Awareness

A formal training program for the employees shall be developed. A process shall be established to evaluate the training requirements for the identified employees. Appropriate training shall be conducted based on the skill set and proficiency of the person to enable them to perform the task.

5.6 Monitor and Review

Any change to the IT asset shall be made only after assessing the implications of the IT recovery readiness.

It shall be ensured that any new application introduced in the IT environment shall have a documented IT DR process based on its criticality and shall integrate with the existing recovery processes.

Any changes that may impact on the recovery procedure shall be duly identified as part of the change control process and shall be approved by the IT DR steering committee prior to implementation.

Any removal or decommissioning of the IT application shall be assessed for its impact on the existing ITDR procedure prior to its signoff.

5.7 Test and Exercise

An ITDR testing framework shall be documented indicating the different types of testing that shall be performed and its frequency.

All IT applications shall be tested based on their classification levels. The frequency of testing shall be documented as part of the ITDR testing framework.

All ITDR tests shall be conducted after careful planning to ensure no disruption to business operations. All risks shall be documented and communicated to all affected people prior to the test.

A clearly defined, documented and approved process shall exist to provide a standardized post-exercise, rehearsal and/or testing evaluation report that is signed off by the application owner.

Detailed test records shall be maintained for all tests that have been conducted. Feedback forms from process owners shall be used to further refine the recovery procedures.

5.8 Continuous Improvement

Procedures for corrective actions shall be developed to provide guidance in the event of a failure to address the following:

1. Identification of failure.
2. Determine the cause of failure.
3. Determine the corrective actions to be taken to recover from the failure.

5.9 Compliance

All relevant statutory, regulatory and contractual ITDR requirements shall be identified and SISL's approach to meet these requirements documented and kept up to date.

Management shall ensure that all ITDR procedures and activities within their area of responsibility are carried out to achieve compliance with the ITDR policy and framework requirements.

Periodic internal audits shall be carried out to verify compliance with the ITDR policy.

6 Reference

Ref: SISL-IT-PRO- BCM Procedure
SISL-IT-PRO-BCP ITDR Plan

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