SISL-IT-POL-Database Security Policy

Version No: V 1.0

INTERNAL DOCUMENT

OCTOBER 2025

Document Control

Document Name	SISL-IT-POL-Database Security Policy
Abstract	This document describes Database Security 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's (SISL) databases hold critical business information and shall be protected at all times.

2 Policy Statement

The databases shall be set up and configured as per industry best practices. Confidentiality, Availability and Integrity of the database shall be maintained at all times. User access to the databases shall be provided after proper authorization and authentication. The access shall be based on the user's role and their job requirement.

3 Scope

The policy applies to

- All the databases
- IT Team

4 Roles and Responsibilities

Sr. No.	Role	Responsibility
1.	Designated Officer (DO)	Ensure that the policy is implemented
2.	Information Security Manager (ISM)	Enforce the policy
3.	IT Team	Implement and abide by the policy for each database instance.
4.	Supplier	Abide by the policy

5 Standards and Guidelines

5.1 Database Naming Convention

Databases shall follow a defined naming convention for easy database identification.

5.2 Database Documentation

All security settings shall be as per access management rights for the database

5.3 File System Security for Database

Databases are installed on operating systems. Database configuration files containing the database configuration and the data are stored in the operating system files.

The Operating system security policy shall apply to the database files stored on the operating system.

It shall be ensured that these files are protected by OS level permissions.

The IT Team shall ensure that the OS level file permissions are documented and implemented.

5.4 Database User Management

User's access to the database shall be governed by the Logical Access Control Policy.

5.4.1 New User Provisioning

User accounts shall be created in the database for application access, database backup, maintenance and optimization.

5.4.2 User Authentication

- All database users shall be authenticated before access is granted.
- Access shall be granted after the user logs in with their own user ID and password.
- Access shall not be provided to user accounts with default / no passwords.
- All database users shall have a unique database ID. The user IDs shall not be shared.
- In case a generic ID is required, proper approvals shall be sought and obtained.

5.5 Database Account Policy

The IT Team shall modify the default user profile to enforce the account policy settings.

The database's user ID and passwords shall be in compliance with SISL's password policy.

5.6 Data Integrity

Integrity of the data in concurrent user mode shall be designed in the database through appropriate mechanism.

5.7 Database Logging

Database logging shall be enabled to track its usage. Audit enables the IT Teams to monitor critical events and functions as an early warning system to detect malicious access attempts. The database shall be configured to log the following events.

- User Account Management
- User Privilege changes
- User login / logout time
- Database configuration changes
- Authentication failures

The database logging shall be governed by the Log Management Policy.

Application owners shall determine the retention period of database logs files. This shall be in compliance with SISL's Data Archival Policy.

5.8 Database Patch Application

IT Team shall ensure that the database is updated with the latest security patches and hot fixes. The patches shall be tested in a test environment prior to deployment in the production environment.

The IT Team shall be responsible for the tracking and testing of the newly released patches.

Patch Management shall be in compliance with SISL's Operating System Security Policy.

5.9 Database Change Management

All changes to the production databases shall be done as per SISL's Change Management Policy.

5.10 Database Incident Management

All incidents related to database security breach shall be logged and shall be governed by SISL's Incident Management Policy

6 Reference

Ref: - SISL-IT-PRO-Logical Access Control Management Procedure

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