# SISL-IT-POL-Log Management and Monitoring Policy

Version No: V 1.0

INTERNAL DOCUMENT

OCTOBER 2025

# Document Control

| | |
|---|---|
| Document Name | SISL-IT-POL-Log Management and Monitoring Policy |
| Abstract | This document describes log management and monitoring 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

A log is a record of the events occurring within an organization's systems and networks. Logs are composed of log entries; each entry contains information related to a specific event that has occurred within a system or network. Many logs within an organization contain records related to computer security. These computer security logs are generated by many sources, including security software, such as antivirus software, firewalls, and intrusion detection and prevention systems; operating systems on servers, workstations, and networking equipment; and applications.

Computer security log management is the process of generating, transmitting, storing, analyzing, and disposing of computer security log data. Log management is essential to ensure that computer security records are stored in sufficient detail for an appropriate period of time. Routine log analysis is beneficial for identifying security incidents, policy violations, fraudulent activity, and operational problems. Logs are also useful when performing audit and forensic analysis, supporting internal investigations, establishing baselines, and identifying operational trends and long-term problems.

# 2 Policy Statement

The Log Management Policy defined by Share India Securities Limited (SISL) functions as a framework for log collection, review, retention and disposal of its computing infrastructure which includes servers, applications, operating system and networking devices.

All devices that have logging capabilities, such as operating systems, applications, firewalls, routers, switches, and so forth, shall be configured to produce a security audit log.

# 3 Scope

The Policy applies to

- IT Team and concerned personnel authorized to configure and review logs for the activities at the Domain, Application and Network Level.
- All critical information assets owned by SISL.
- All Networking devices like firewalls, switches, wireless access controllers and wireless access points.
- All business-critical applications
- Operating Systems on business-critical servers
- Access Control by third party vendors to SISL's IT computing environment.
- Remote Access via VPN to SISL's environment.
- Business Critical laptops / desktops

## 3.1 Scope Exclusions

Workstations, PBXs, smart phones, are not in the scope of this document.

# 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. | IT Team | Adhere to the policy |

# 5 Standards and Guidelines

## 5.1 Monitoring networks, systems and applications

SISL shall monitor networks, systems and applications for anomalous behaviors and appropriate actions shall be taken to evaluate potential information security incidents.

The monitoring scope and level determined by SISL shall be in accordance with business and information security requirements and taking into consideration relevant laws and regulations. Monitoring records shall be maintained for defined retention periods.

SISL shall consider the following within the monitoring system:

- Outbound and Inbound network, system and application traffic.
- All levels of access to systems, servers, networking equipment, monitoring system, critical applications, etc.
- Critical or admin level system and network configuration files.
- Logs from security tools.
- Event logs relating to system and network activity.
- Checking that the code being executed is authorized to run in the system and that it has not been tampered with (e.g. by recompilation to add additional unwanted code).
- Use of the resources (e.g. CPU, hard disks, memory, bandwidth) and their performance.
- SISL shall establish a baseline of normal behavior and monitor against this baseline for anomalies.
- SISL shall consider the following when establishing a baseline:
    - Reviewing utilization of systems at normal and peak periods.
    - Usual time of access, location of access, frequency of access for each user or group of users.

- The monitoring system shall be configured against the established baseline to identify anomalous behavior, such as:
  - Unplanned termination of processes or applications.
  - Activity typically associated with malware or traffic originating from known malicious IP addresses or network domains (e.g. those associated with botnet command and control servers).
  - Known attack characteristics (e.g. denial of service and buffer overflows).
  - Unusual system behavior (e.g. keystroke logging, process injection and deviations in use of standard protocols).
  - Bottlenecks and overloads (e.g. network queuing, latency levels and network jitter).
  - Unauthorized access (actual or attempted) to systems or information.
  - Unauthorized scanning of business applications, systems and networks.
  - Successful and unsuccessful attempts to access protected resources (e.g. DNS servers, web portals and file systems).
  - Unusual user and system behavior in relation to expected behavior.

SISL shall deploy a monitoring tool for continuous monitoring. Monitoring shall be done in real time or at periodic intervals, subject to organizational need and capabilities. Monitoring tools shall include the ability to handle large amounts of data, adapt to a constantly changing threat landscape, and allow for real-time notification. The tools shall also be able to recognize specific signatures and data or network or application behavior patterns.

Automated monitoring software shall be configured to generate alerts (e.g. via management consoles, email messages or instant messaging systems) based on predefined thresholds. The alerting system shall be tuned and trained on the organization's baseline to minimize false positives. Personnel shall be dedicated to responding to alerts and shall be properly trained to accurately interpret potential incidents. There shall be redundant systems and processes in place to receive and respond to alert notifications.

Abnormal events shall be communicated to relevant parties in order to improve the following activities: auditing, security evaluation, vulnerability scanning and monitoring. Procedures shall be in place to respond to positive indicators from the monitoring system in a timely manner, in order to minimize the effect of adverse events on information security. Procedures shall also be established to identify and address false positives including tuning into the monitoring software to reduce the number of future false positives.

## 5.2 Auditing

Auditing is a means of tracing the activities carried out by users and applications. Operating systems, databases and applications shall be configured to audit the transactions that meet exceptional criteria. It shall be ensured that these transactions are completely and accurately highlighted.

Logs and Audit trails are a means of recording a user's or system activity as it happens. This helps in tracing systems generated faults or errors caused by humans. However, logs and audit trails do not prevent the events from occurring. If publicized as an ongoing security practice, this may deter the misuse of system resources.

Adequate audit trails shall be captured, and certain information needed to determine sensitive events and pattern analysis to indicate possible fraudulent use of the system (e.g. repeated unsuccessful logons, access attempts over a number of days) shall be analyzed.

This audit trail shall include information on who, what, when, where, and any special information such as

- Success or failure of the event
- Use of authentication keys, where applicable

The IT Team shall identify the events and activities to be audited and logged.

The specific list of events to be audited shall depend on the security requirements identified during the system setup process as defined in the operating system security policy. At a minimum, the system shall audit all user logins and any privileged activities.

### 5.2.1 Who will log

Any user carrying out critical activities or accessing systems that hold sensitive information shall be identified and tracked.

### 5.2.2 What to log

The following logs shall be monitored -

- Logs of System Activity.
- Logs of User's Access.
- Logs for Network Monitoring.
- Logs of Server Performance Monitoring.
- Logs of Antivirus / Threat Intelligence activities.
- Logs for Patch Management

The following events shall cause a record to be written to the security audit log:

- Successful or failed user authentication attempts.
  - All identification information shall be logged, even if the user ID supplied is not valid.
  - Plaintext passwords may not be logged; passwords that are disguised by asterisks or another similar mechanism may be logged.
- Resource access attempts denied by the resource access control mechanism.
- Successful accesses of security critical resources (e.g. Secret data, screen routers, firewalls, intrusion detection systems (IDS), etc)

- Creation, modification or deletion of critical or sensitive files or database information. Note: the extent of such logging will be determined by each system, application or data owner
- Changes to the set of privileges associated with a user.
- Changes to the access rights of resources
- Changes to system security configurations (for e.g. firewall rules, IDS rules, new system accounts, etc)
- Modification of system-supplied software (e.g. application files, services, registry settings, etc)

### 5.2.3 When to log

The ISM (Information Security Management Team) shall define the period for which auditing needs to be enabled on a system.

### 5.2.4 Where to log

Audit logs may be recorded on the host that generates the logs. When the host generating the audit log is different from the host recording it, the path between them shall be secured. To protect the audit logs on the logging host, the audit logs shall be "read only" from the logging host console.

Auditing and logging for the identified events and activities shall be enabled on

- Mail Server
- Database
- Applications
- OS

Proper selection of audit events requires a careful balance between capturing all the information that may provide clues to user actions and system performance.

If too many events are captured, system performance may be too slow, and the audit logs shall be large but may not yield any useful information. Where enough events are not captured, a critical piece of information required to identify an event, attacker, or even to notice a system break-in may be missed.

## 5.3 Audit Trail Protection

It is particularly important to ensure the integrity of audit log data against modification. Access to audit log files shall be protected (for example: file or folder permissions, access control rules, etc.) Only authorized users shall access utilities that can reconfigure audit logs, turn the audit logs on and off, and write to, modify, and read audit log data. Intruders shall not be able to remove or alter signs of an intrusion or add erroneous information. Controls shall aim to protect against unauthorized changes and operational problems including:

- Deactivating any audit logs

- Alterations to the recorded message types
- Audit logs being edited or deleted
- Audits log media becoming exhausted, and either failing to record events or over-writing itself.

In the event of a security breach that has been logged as an audit event, care shall be taken to protect the evidence as mentioned in the Incidence management policy.

Audit-trails shall be backed up daily along with the regular back-ups that are taken. These backups shall follow the backup and recovery policy.

## 5.4 Log Backup and Archival

The following backup and archive activities shall occur for all audit log files on applications or systems that conduct regular backups:

- Audit log files shall be captured as part of the regular SISL backup procedure. Audit log files may be stored onsite or offsite depending on the regular backup procedure.
- Audit log files shall be backed up before being overwritten or reset manually by authorized personnel or automated tools.

## 5.5 Log Retention

Audit log files shall be retained, either onsite or offsite, and accessible based on access control policy and stored on secured storage devices. Audit trails shall be retained for a minimum period of 365 days but may be retained longer if the system being logged is particularly critical or high risk. Records, which are of legal nature and necessary for any legal or regulation requirement including DPDP or investigation of criminal behavior, shall be retained as per the requirements of law.

When media containing audit log data are no longer needed, they shall be securely disposed of (e.g. shredding hardcopy output, sanitizing removable media, destroying CD-ROMs). The disposal shall be in compliance to the Asset Disposal Policy.

## 5.6 Log and Audit Controls

Controls shall be implemented so that operational problems do not occur with the logging facilities. It shall be ensured that unauthorized changes are not made to the logging facilities and to the logs. The following shall be considered and ensured.

- Logging facilities are not deactivated.
- Message types that are recorded are not altered.
- Log files are not edited or deleted.
- Log file media do not get exhausted, fail to record events and overwrite itself.

## 5.7 Log Review

A team shall be identified to monitor logs in a regular basis. The team shall report to the DO. Identified incidents shall be immediately reported to the respective teams.

Automated or manual procedures shall be used to monitor and promptly report all significant security events, such as accesses, which are out-of-pattern relative to time, volume, frequency, type of information asset, and redundancy.

Reviewers shall know what to look for to be effective in spotting unusual activity. They need to understand what normal activity looks like. Audit log review can be easier if the audit log function can be queried by user ID, terminal ID, application name, date and time, or some other set of parameters to run reports of selected information.

***Audit Log Review after an Event*.** Following a known system or application software problem, a known violation of existing requirements by a user, or some unexplained system or user problem, the appropriate system-level or application-level administrator shall review the audit logs. Review by the application/data owner would normally involve a separate report generated by the system administrator, based upon audit log data, to determine if their resources are being misused.

***Periodic Review of Audit Log Data*.** Periodic audit log reviews are encouraged. Application owners, data owners, system administrators, and computer security administrators shall determine how much review of audit logs is necessary, if any, based on the importance of identifying unauthorized activities, and who shall conduct the reviews. This determination shall have a direct correlation to the frequency of periodic reviews of audit log data.

The following chart designates a *suggested* audit log review frequency according to the type of data involved.

| Types of Data | Review Frequency |
|---|---|
| Public | Quarterly |
| Internal | Monthly |
| Confidential | Weekly |
| Threat Intelligence Critical Logs | Immediately |

All events that indicate a security breach shall be acted upon as per the incidence management policy.

## 5.8 Enhancing Security Monitoring

SISL shall enhance security monitoring of its networks, systems and application by:

- leveraging threat intelligence systems or

- leveraging machine learning and artificial intelligence capabilities; or
- Using blocklists or allowlists; or
- Undertaking a range of technical security assessments (e.g. vulnerability assessments, penetration testing, cyber-attack simulations and cyber response exercises), and using the results of these assessments to help determine baselines or acceptable behavior.
- Using performance monitoring systems to help establish and detect anomalous behavior.
- Leveraging logs in combination with monitoring systems.

Monitoring activities are often conducted using specialist software, such as intrusion detection systems. These can be configured to a baseline of normal, acceptable and expected system and network activities.

Monitoring anomalous communications helps in the identification of botnets (i.e. set of devices under the malicious control of the botnet owner, usually used for mounting distributed denial of service attacks on other computers of other organizations). If the computer is being controlled by an external device, there is a communication between the infected device and the controller. SISL shall therefore employ technologies to monitor anomalous communications and take such action as necessary.

## 5.9 Incident Reporting

Any incidents shall immediately initiate the Incident Management Process as defined in the Incident Management Policy.

Monitoring team shall classify the incident based on

**High Risk** – All logs that can cause direct harm to the system including buffer overflows, denial of service attacks, super user logins and changes to critical system files.

**Medium Risk** – All logs that relate to activities that may lead to an attack including port scanning and vulnerability scanning.

The Information Security Team shall work with the respective system / network / database / application administrator towards the closure of this incident.

## 5.10 Change Management

Any changes to the log collection configuration shall be done only after a change request for the same has been raised. This shall be in compliance with the Change Management Policy.

# 6 Appendix

## 6.1 Activities to Log

The following are examples of different types of users, audit, network, process, and admin activities that shall be logged, as applicable. Events can be logged at the application level, operating system level, or network level depending on the activity.

### 6.1.1 User Activity

These logs are currently saved on the local machines.

- Successful login
- Logout
- Successful password change
- Unsuccessful password change

### 6.1.2 Operating System Logs

The following event shall be captured on an operating system.

- Successful and rejected system access attempts.
- Successful and rejected data and other resource access attempts.
- Audit trails of all privileged accesses.

### 6.1.3 Process Activity

- Successful program activation
- Unsuccessful program activation
- Normal program completion
- Abnormal program completion
- Failed attempts by internal system accounts
- Successful login / log off

### 6.1.4 Network Device Logs

The network device logs shall cover the below mentioned details.

**Router Logs**

- Network Traffic
- SNMP Traps
- Console Logging
- Configuration Change Logs
- Unauthorised Access
- Inbound and Outbound packets which have been dropped

**Switch Logs**

- Network Traffic

- SNMP Traps
- Console Logging
- Configuration Change Logs (If Facility Available)
- Unauthorised Access
- Inbound and Outbound packets which have been dropped

**Firewall Logs**

- Changes to network interfaces
- Addition/deletion/changes of administrative accounts
- Unauthorised Access
- Dropped inbound and outbound packets.
- Successful modification of firewall rules
- Unsuccessful modification of firewall rules
- All dropped packets, denied connections and rejected attempts
- Inbound authorized connections from the Internet to the DMZ
- Authorized connections from the DMZ to the internal network
- Outbound authorized connections from the internal network and the DMZ
- Traffic to/from 3rd Party Segment
- Authorized Connections within the internal network
- Any error messages from the firewall system and routers where possible

**Wireless Controllers and Access Points**

- Wireless Devices connected to the AP
- The network traffic across the wireless controllers and AP.
- Configuration changes
- Unauthorised Access
- Rogue AP's

**Intrusion Prevention / Detection System (IPS / IDS)**

- Successful Login / Log off
- Intrusion Alerts
- Configuration Changes
- Console Alerts

**Audit Activity**

- Successful log rotation
- Unsuccessful log rotation
- Successful audit configuration changes
- Unsuccessful audit configuration changes
- Logs filling
- Successful enabling of auditing

- Successful disabling of auditing
- Unsuccessful attempt to disable auditing

## 6.2 Activities to Monitor

The following are examples of different types of users, audit, network, process, and admin activities that shall be monitored, as applicable, if monitoring is being conducted. Activities can be monitored at the application level, operating system level or network level depending on the activity. The threshold for repeated activity should be 5 in a period of 5 minutes (for example, 5 unsuccessful login attempts for the same user or many different users within 5 minutes).

### 6.2.1 User Activity

- Repeated unsuccessful login for same user or many different users
- Repeated unsuccessful login with different wrong user id
- Repeated unsuccessful login to a disabled, expired or locked account
- Repeated unsuccessful password change for same user or many different users
- Unsuccessful login attempt to a server, without right to log in locally
- Repeated unsuccessful access to the same or different sensitive objects for the same user
- Successful access to sensitive object by unauthorized user
- Unsuccessful change to content or privileges of a system configuration file
- Successful change to content or privileges of a system configuration file
- Repeated unsuccessful object access
- Repeated unsuccessful object deletion

### 6.2.2 Audit Activity

- Failure to properly escalate monitor alerts
- Presence of “unexplained periods” without logged events. The amount of time would depend on the normal pattern of logged events.
- Corruption of event logs
- Successful changes in audit configuration in an “unusual window”
- Unsuccessful changes in audit configuration
- Unsuccessful attempt to disable auditing
- Successful disabling of auditing
- Successful manual log deletion
- Unsuccessful log rotation
- Audit log space filling

### 6.2.3 Network Activity

- Repeated unauthorized attempts to login via remote access to the firewall

- Outbound authorized connections from the internal network and the use of unusual ports
- Any traffic, which attempts to initiate a connection from the DMZ to the internal network
- External traffic with internal spoofed IP addresses
- Internal traffic with external spoofed IP addresses
- Successful firewall rules change in an “unusual window”
- Repeated unsuccessful modification of firewall rules

### 6.2.4 Process Activity

- Termination of intrusion detection process or other security tools process
- Failed attempt to log with an application or system account
- Processes consuming excessive resources (wall clock time, CPU time, memory, disk)

### 6.2.5 Admin Activity

- Repeated unsuccessful administrative login
- Administrator account locked out
- Administrator access to sensitive data
- Administrator access to user data
- Account Policy compliance for administrators: use of su to access root
- Account Policy compliance for administrators: use of su to access root by a normal user
- Repeated unsuccessful object ownership modification
- Repeated unsuccessful user privilege modification
- Repeated unsuccessful user creation or deletion
- Creation and Deletion of the same user in a short period
- User account added to administrator group in an “unusual window”
- Administrative privileges granted to a user or group in an “unusual window”
- Unsuccessful change to the Account Policy
- Successful change to the Account Policy in an “unusual window”
- Unsuccessful time system modification
- Unsuccessful scheduler modification
- Unexpected shutdowns, reboots and restarts

# 7 Reference

Ref: SISL-IT-PRO- Log Management Procedure

# 8 Policy Review Frequency

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

# 9 Policy Exception

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

# 10 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 |