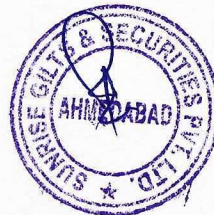


**SUNRISE GILTS & SECURITIES PRIVATE LIMITED**

**LOGGING AND MONITORING POLICY**

(EFFECTIVE DATE: 10/06/2025)



<b>Author:</b>	PRATIK KUMAR MORE
<b>Owner:</b>	PRATIK KUMAR MORE
<b>Approved by:</b>	BOARD OF DIRECTORS
<b>Organization:</b>	SUNRISE GILTS & SECURITIES PRIVATE LIMITED
<b>Version No:</b>	1.1
<b>Approval Date</b>	28/05/2025
<b>Effective Date:</b>	10/06/2025

## Document Control

Document Title Logging and Monitoring Policy

## Version History

Version No.	Version Date	Author	Summary of Changes
1.0	13/06/2019	PRATIK KUMAR MORE	NA
1.1	10/06/2025	PRATIK KUMAR MORE	Review and Approval of BOD





## Approvals

Name	Title	ApprovalDate	Version No
PRATIK KUMAR MORE	Logging and Monitoring Policy	13/06/2019	1.0
PRATIK KUMAR MORE	Logging and Monitoring Policy	28/05/2025	1.1

### 1.0 LOGGING AND MONITORING POLICY

#### 1.1 PURPOSE

- IT infrastructure components forms a crucial part of SUNRISE GILTS & SECURITIES PRIVATE LIMITED operations. IT assets are constantly under threat from malicious users and as a result, needs to be monitored effectively on a continuous basis for any abnormal activities. This policy aims to establish effective system to centrally log and monitor information security controls.

#### 1.2 SCOPE

This policy applies to:

- All staff and non-employees, stakeholders (interns, contractors, consultants, suppliers, vendors etc.) of *SUNRISE GILTS & SECURITIES PRIVATE LIMITED* and other individuals, entities or organizations that have access to and use *SUNRISE GILTS & SECURITIES PRIVATE LIMITED*' information processing systems and card holder data environment to perform their daily job-related responsibilities or meet their contractual obligations.
- All Information assets involving data, applications, network, security devices, servers and other IT system

#### 1.3 POLICY STATEMENTS

Logging shall be enabled on all information processing assets. All access to critical applications and *SUNRISE GILTS & SECURITIES PRIVATE LIMITED*' network shall be logged and monitored for suspicious activities or security breaches and adequate response mechanism shall be setup for controlling security breaches.



### 1.3.1 LOG MONITORING

- Logging shall be enabled for all the critical devices including application servers, network devices and security devices.
- The logs of the applications shall be monitored periodically to ensure proper functioning and policy compliance.
- Some of the following activities and parameters shall be logged and monitored, but not limited to:
  - Access to all audit trails
  - Initialization of audit logs
  - Stopping or pausing of audit logs
  - Remote access activities of vendors
  - All individual access to cardholder data
  - Actions taken by any individual with root or administrative privileges
  - Invalid logical access attempt
  - Identification and authentication mechanisms
  - Creation and deletion of system level objects
- Parameters related to audit trails:
  - Ensure user identification is included in log entries
  - Ensure type of event is included in log entries
  - Ensure date and time stamp is included in log entries
  - Ensure success or failure indication is included in log entries
  - Ensure that audit trails are enabled and active for system components
  - Ensure ONLY individuals who have a job related need, can view audit trail files. Access to audit trail files shall be monitored regularly
  - Ensure current audit trail files are promptly backed up to a centralized server or media that is difficult to alter
- The logs shall be analysed for the following:
  - Unauthorized access
  - Configuration changes
  - Abnormalities in mail routing events
  - Failed logins





- o Denial of service attempts

#### 1.3.2 INCIDENT REPORTING

- Any incident shall immediately initiate the IT Incident Management Process as per the IT Incident Management Policy.
- Designated Officer shall prepare the "Log Analysis Report", post any event identified.

#### 1.3.3 BACKUP

- Logs in the centralized server shall be backed up on a periodic basis.
- The backup logs shall be protected from unauthorized access.
- The Retention period of the logs shall be decided by the Designated Officer. Though all logs shall be maintained for minimum period of 1 year.

