ARYA FIN-TRADE SERVICES (INDIA) PRIVATE LIMITED

Audit Trail Policy

Version	**2024/01.02**
Review Date	**05/04/2024**
Review & Approved by	**Reviewed by Technology Committee & Approved by Board of Directors**

1 Overview

The Audit trails maintain a record of all actions on resources by Individuals and computing programs and processes.

2 Purpose

The purpose of the policy is round the clock tracking of resource usage, detailed monitoring of employee activity, real time event logging and so on.

3 Policy

3.1 The functions that shall be recorded are; log-in attempts, password changes, file creations, changes and/or deletions and so on.

3.2 The audit trail event record shall specify type of event, occurrence of event, user ID associated with the event and program or command used to initiate the event.

4 Component of Audit Trail Policy

The following are the components of the audit trail policy:

4.1 A regular back-up of the audit log files shall be taken to fix the accountability for usage of resources on individuals, enable reconstruction of events, intrusion detection and enable analysis of problems and failed events.

4.2 Audit trails shall be reviewed on a regular basis and corrective action shall be taken based on audit trail information.

4.3 A proper register shall be maintained for the back-up of the audit trail and the person responsible shall put his initials on it.

5 Review

Audit trails shall be reviewed weekly by the Security Officer or other authorized individuals or who do not administer access to the database. Management must review the audit trail monthly.

6 Reporting

Anomalies shall be immediately reported to appropriate supervisory and/or management for follow-up action. In case of anomalies of serious nature a committee shall be set up for further investigation. The relevant department head shall be a part of the Investigating Team. In case of the scrutiny of activities of the department head, any other person designated by the Managing director shall be a part of the investigating team.

7 Compliance

Unauthorized personnel are not allowed to verify or obtain sensitive data. The gross negligence or willful disclosure of information shall result in prosecution resulting in fines and/or dismissal.

8 Storage

All audit files shall be stored in a locked room and kept for ten years.

9 Review and Update

This policy shall be reviewed and updated on an annual basis or on any special event or circumstance.