NAME OF THE STOCKBROKER

AUDIT TRAIL POLICY

POLICY CONTROL

Version:	1.0
Version Date:	_____ (Date of Passing Board Resolution)
Approved by:	Board of Directors
Department in Charge:	
Frequency of Review:	Yearly or as and when any update comes change in the Relevant Regulation comes or any change in the Company's internal control or Structure whichever is earlier.

TABLE OF CONTENTS:

AUDIT TRAIL POLICY

I. OVERVIEW:

Audit trails maintain a record of all actions on resources by individuals and computing programs and processes. Audit Trail Policy is intended to ensure that computers and network devices have proper logging to detect, investigate, and remedy events that may be a security hazard or a threat to the organization or personnel.

II. PURPOSE:

The purpose of this policy is to ensure that critical systems, access control devices, network events etc. are being recorded and periodically monitored, and proactive measures are taken to ensure continued security and availability of the key systems.

III. POLICY:

The following are the components of the audit trail policy:

- This policy states all information systems logs/audit trails are to be reported promptly and recorded. Error logs, privileged user logs should be properly reviewed and managed to ensure the system security.
- A regular back up of the audit log files should 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.
- Audit trails should be reviewed on a regular basis and corrective action should be taken based on information gathered. Only authorized teams should have access to those audit trail files.
- All login and logout events on servers, applications, all devices, domains should be logged.
- Logs should be maintained for all physical access control devices that control access to secure areas.
- Audit trails should be maintained for all the security events including but not limited to following parameters:
  - Access to critical systems
  - Use of and changes to identification and authentication mechanisms
  - Creation of new accounts and elevation of privileges
  - Creation and deletion of system level objects
  - Success and failure of logical access attempts
  - Access to all audit trails

- Changes to system configurations
- Changes, additions, or deletions to accounts with root or administrative privileges
- Changes to network configurations

- All the audit trails should be protected against tampering and unauthorized access. Alert notification should be sent to the respective personnel for unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files for taking corrective actions further.
- A proper register should be maintained for the back up of the audit trail and the person responsible should put his initials on it.

IV. CLARIFICATION/INFORMATION:

In case of any clarification/information required on the implementation of the Policy, please contact the IT Head/Compliance Officer on Email -_____, Tel No._____.

V. REVIEW:

The said policy shall be reviewed by the Board of the Directors on a yearly basis or as and when any update comes change in the Relevant Regulation/Circular comes or any change in the (Name of the Stock Broker)'s internal control or Structure. The Compliance officer has the authority to give direction to undertake additions, changes, and modifications, etc. to this Policy, and the same shall be effective per the authority of the Compliance Officer and thereafter be ratified by the Board of the Directors at its next review.

X-X-X-X-X