NAME OF THE STOCKBROKER

ASSET MANAGEMENT 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:

USER MANAGEMENT POLICY

I. BACKGROUND:

The organization identifies inventory management groups with the objective of creating and maintaining inventory of servers, applications, network devices, workstations/laptops, software licenses & any other asset that is critical to the organization.

- 'Identify' critical IT assets and risks associated with such assets.
- 'Protect' assets by deploying suitable controls, tools and measures.

The inventory of assets has at least the following details:

- Asset Name and Description
- Asset Purchase/Warranty Information
- Asset Location
- Nominated Owner & Custodian of the asset

II. ASSET CLASSIFICATION:

Assets for IT Department is grouped under the following asset types for the inventory purpose:

- Physical assets
- Software assets
- Services assets
- People assets
- Paper/Softcopy assets

All paper/Softcopy assets carry the classification on them. The following classification criterion is followed:

Classification Level	Definition	Examples
Confidential	Applies to less sensitive business information, the unwanted disclosure of which can bring substantial financial damage, or damage to the company's reputation. Confidential information is important information determining the technical or financial success of parts of the company. This especially applies to information which can be of value to competitors.	• Personnel data, e.g. assessment documentation, and data which must be handled in accordance with the protection laws; • Confidential information about third parties (in particular within the context of secrecy agreements); • Information on security measures and serious deficiencies, information on internal network topology; • Copies, backups and archives of confidential information; These examples might also require higher classifications.
Restricted	Applies to business information for which unwanted disclosure to outsiders can have damaging consequences. This is generally information which is accessible to a wide circle of employees but is not intended for outsiders	• Internal communications, internal e-mails, correspondence, Content on Intranet. • Internal guidelines, like circulars, instructions, organization plans • Internal information like contracts, reports, plans
Unclassified	This classification applies to information, which has been explicitly approved by the management for release to the public. By definition, there is no such thing as unauthorized disclosure of this information and it may be freely disseminated without potential harm.	• Product brochures • Content on website • Advertisements • Press releases

All documents older than the release date of this policy or as decided by the Information Security Group and formally communicated, may not be tagged immediately. All documents created or accessed after the said date need to be tagged by the document owner according to the classification given and handled accordingly.

III. ASSET LABELLING:

- Classified assets covered under scope are labelled to ensure that they are given necessary protection in use, storage and transport.
- Physical items contain the physical classification label on them.
- Documents and information have the classification mentioned on them.

IV. ASSET HANDLING:

- For each classification, handling procedures is defined to cover the following types of information processing activities:
    - Copying
    - Storage
    - Transmission by post, fax and electronic mail
    - Transmission by spoken word including mobile phone, voice mail, answering machines
    - Destruction

V. INFORMATION/ SOFTWARE EXCHANGE:

- When information is exchanged between two parties with the use of information exchange equipment like mobile, electronic mail, Internet etc., following controls is considered
- While using a mobile phone in a public place, ensure that the information is not overheard by any unauthorized person.
- While sending any confidential information via courier, ensure that it is covered and sealed in a tamper-proof envelope.

VI. 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._____.

VII. 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