NAME OF THE STOCKBROKER

MEDIA HANDLING AND SECURITY 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:

Sr. No	Particulars	Page No
1.	Scope	4
2.	Purpose & Objective	4
3.	Management of Removable Computer Media	4
4.	Disposal Procedure	4
5.	Laptop/Desktop Handling Procedure	5
6.	Information Handling Procedure	5
7.	Security of System Documentation	6
8.	Clarification/Information	6
9.	Review	6

MEDIA SECURITY AND SECURITY POLICY

I. SCOPE:

The aim of this policy is to sets out practices to be followed for ensuring the information, storage media and other information containers should be handled in proper and secure manner to reduce the risk of unauthorized people stealing or misusing company's internal, secret or confidential information. This is applicable to all employees, board members, temporary employees, vendors, and contracted staff of company.

II. PURPOSE & OBJECTIVE:

Information is a valuable asset and consequently needs to be rightfully protected. The purpose of this policy is to prevent any kind of damage or compromise of assets that may cause interruption to the business activities.

III. MANAGEMENT OF REMOVABLE COMPUTER MEDIA:

Following controls should be in place to control the information on any removable media (if used):

- Any person copying data on removable media should keep such media secured.
- If the data on such removable media is no longer required, the contents should be erased.
- All removable media in desktops should be disabled and physically removed wherever possible.
- Removable media should be allowed only to those systems which are approved by IT Team.
- Proper disposal methods should be used as explained in next section to dispose such media when not required.
- All media if used should be stored in a safe, secure environment, in accordance with manufacturer's specifications.
- All the removable media should be encrypted to protect from unauthorized access.

IV. DISPOSAL PROCEDURE:

- Items which may require secure disposal include paper documents, output reports, removable hard disks and system documentation etc.
- Following disposal methods should be used for disposing of several types information.

- Printed materials/paper documents: All paper should be disposed of by shredding.
    - **Removable Media:** when media is worn, damaged or no longer required then it should be disposed of in a secure manner to prevent the compromise of sensitive information.
    - **Hard Disk:** If any old PC/laptop is removed out of the premises; the hard disk of those computing systems should be formatted before it is disposed. Same should be done for any other hard disks. If the hard disk is damaged and cannot be detected; such hard disk should be physically damaged and burnt. Memo should be retained with required approvals either from Leadership Team OR ISF Team Member.
    - **Equipment:** Admin and facility team has to ensure equipment productivity after its depreciation period. If the equipment is not functioning to meet the business requirement of company, then Admin and facility team can take a call to scrap/donate/sell the equipment. The equipment's memory element has to be damaged beyond repair and other parts can be disposed of by destroying them or sending them for recycling. In case of donating/selling the equipment, it has to be ensured that the memory elements of the equipment are formatted thoroughly and tested to see if data can be still retrieved. If it is possible to retrieve data, the equipment's memory elements should be removed, and the rest of the equipment can be donated. Memo should be retained with required approvals.

V. LAPTOP/DESKTOP HANDLING PROCEDURE:

In case of employee exit, backup of information reside on laptops/desktops should be taken by respective project managers and those systems should be formatted by outsourced party post authorization and approvals from the IT team.

VI. INFORMATION HANDLING PROCEDURE:

The following measures shall be considered:

- All the sensitive and confidential information in electronic format shall be kept in the centralized server OR centralized repository for ease of retrieval and security.
- All confidential information in form of paper shall be kept under lock and key with the proper procedures describing access controls.
- All information either in soft or hard form, must be labeled as per the information classification defined.
- All information labeled as confidential and sensitive, must have access list for authorized person who can access this information.
- All information which is not labeled must be considered as "Internal" and should not be shared with customers or any external person who has not signed NDA with company.
- Distribution of sensitive and confidential information should be kept to minimum required.

- The owner of the information should monitor all printing and faxing of information personally. Owner should ensure the process is complete and no document is left behind on the printer.
- If the print job or faxing is stopped in between due to any problems, owner should ensure that the problem is solved and all data in the spool is cleared.
- Access restriction of sensitive and confidential information shall be reviewed.

VII. SECURITY OF SYSTEM DOCUMENTATION:

- Following systems documentation should be created and maintained securely by the system administrator / IT Team for each system.
    - System configuration details
    - Change history
    - Access authorization process and access list
    - Procedures to be followed for regular maintenance of the system
    - Backup details
    - Disaster recovery plan & DR responsibilities for the system
    - Third party support contracts etc.
- All above documents should be updated regularly when any change is made.
- All above documents should be classified as confidential and the access list should be kept to minimum authorized by the system owner.

VIII. 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._____.

IX. 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 directions 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. Periodic audits will be conducted to ensure compliance with this policy.

X-X-X-X-X