NAME OF THE STOCKBROKER

INFORMATION 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:

INFORMATION SECURITY POLICY

I. OBJECTIVE:

This document outlines the policy and procedures for information system security. Information security is the collective processes put in place to ensure the safety, integrity, and privacy of a piece of information and data.

II. PURPOSE:

The information security policy document is the backbone of the organization and it sets the foundation and framework for security of information and information systems, mechanisms, procedures and practices at various levels in the organization. It protects hardware, software, data, information, network, computing devices, users and clients from potential security breaches through their use of the firm's resources or services.

III. SCOPE:

This procedure is applicable to and covers the following:

i. All full-time employees and consultants/contractors working under supervision of IT function.
ii. All systems and business applications of the company, which access, process or have custody of corporate information regardless of their location or the media on which it is available.
iii. Computer center, application servers, networks, PC's and laptops.
iv. Information on computer files, on paper or any other media.

IV. PROCEDURE:

The areas covered are:

1. Physical access security procedure.
2. Logical access security procedure
3. External access security procedure

V. PHYISCAL ACCESS SECURITY PROCEDURE:

1. Server Room:

- The physical access to the computer room will be available only to the IT Operations, Authorized Staff and pre authorized Vendor Support Engineers and system auditors.
- The access to the computer room is controlled through access cards and a manual log of entry and exits is maintained.
- Any up gradation or replacement of hard disk on the servers is to be done in the presence of the IT Operations team and any hard disk removed from the server which the vendor wants to carry back is totally formatted or initialized. If there is any system break down and the vendor's physical support is needed then the maintenance work needs to be done in the presence of the IT administrator.

2. Personal Computers/Laptops:

- The prime responsibility of the safety and security of the workstations on the employee's desk lies on the users. This responsibility extends to the official working hours or for the period the employee is within the office premises after which the office security personnel are entrusted with the responsibility. The individual users are expected to report any mishaps or abnormalities related to their system to the IT Operations staff immediately.
- A proper asset register is to be maintained to identify PC and the user using the same. The asset register must also record the IP address of each machine.
- The IT Operations team should authorize any hard disk replacement and the disk should be formatted before sending back to the vendor.

VI. LOGICAL ACCESS SECURITY PROCEDURE:

Protection of the computers, networks and application systems and the information handled by them is an essential part of doing business.
User must manage and maintain access to information in its computer environment by means of an identification and authentication mechanism
A strict password policy should be in place.
The application and network security access assigned to each individual user must be restricted on a need-to-know basis.

1. User Password:

A separate password policy is framed in this regard.

Process for Granting or Revoking System Privileges:

- A request for new user ID's or changes to access privileges granted to existing user ID's must follow the formal request process. All user ID request records must be retained on record for at least a year. The access privileges are granted to the user by software department head. The email account for the new user is created by the operations head.

- Management must re-evaluate user access privileges at least once in a year. Security administrators will issue lists of all users and their associated privileges to department managers for review. Managers will record all required changes on these lists and return them to the security administrators who will revoke all privileges no longer required by individual users.
- There must be a process to review all user ID's that are inactive for 90 days for possible suspension. User ID's inactive for more than 360 days will be disabled.

2. **Server Admin Security:**
   - A user once connected on the server will be automatically mapped to his data area on the server and should not be able to view anything else other than his files. A separate access control list is maintained which specifies the access privileges granted to the employees.
   - Anti-virus scan should be scheduled which will scan the entire hard disk.
   - For creating new logins and mail ID's a request for the same must come from Department Head. Similarly on exit of an employee Department Head must intimate IT Operations Head to delete the logins and mail IDs.

VII. EXTERNAL ACCESS SECURITY PROCEDURE:

All external access to the company must adhere to the following guidelines:

- All users of external connections must be appropriately authenticated and authorized. External connections i.e. remote access is given to the authorized vendors through VNC for support purposes.
- All connections between the company and the Internet or any other public network must transverse the firewall.
- Accounts used for external access must be limited to identifiable individuals.

VIII. IS PROGRAM:

1. **Management Responsibility:**

- The senior management should ensure that proper policies and procedures are in place and the employees adhere to them.
- The management should have an access control procedure to ensure that the data relevant to a particular user is available to them.
- The duties and responsibilities of all the employees should be clearly defined.

2. **Employee Responsibility:**

- The employees should change their passwords at the time interval specified and should not reveal their password.
- All the communication made through e-mails should be for professional reasons and confidential information should be sent in an encrypted form.
- The employees should ensure that their terminals are scanned for viruses and the results should be communicated to the IT Department.

- The employees should restrain themselves from visiting, viewing or downloading pornographic materials from the Internet.
- The employees should follow the rules, regulations and procedures set by the organization.
- The employees should avoid transmission of non-public customer information and should ensure that the information transmitted is delivered to the authorized person who is eligible to receive it for legitimate purpose.
- Information security training should be provided to the employees on the technology used and the job assigned.
- External media such as disks, CDs, tapes should be scanned and should be certified by the IS Department.
- Vendors and Consultants should not be allowed to run their demonstrations and presentations on organizational systems.
- All new software acquisitions should follow a controlled procedure and should be tested for viruses.
- Patches to operating systems and other software and upgrades should be acquired from authentic sources and scanned before installation
- The back-up media should be should be scanned to ensure that viruses do not infect it. The back up media is stored safely in line with the risk involved.

IX. PROCEDURE FOR DATABASE, SYSTEM AND APPLICATION-LEVEL PASSWORD STORAGE:

The database access should be restricted to authorized person and there should be no sharing of passwords. A procedure has to be set to ensure that there is no unauthorized access to confidential and sensitive data. Access to database, applications should be approved by a proper authority.

X. ACTION FOR BREACH OF SECURITY:

The designated person should inform the IT Department in the event of any security breach or compromise reported in the respective department. The IT department should then investigate the matter and inform the senior management. The management would then decide on the course of action to be taken.

XI. EXTENSION OF IS POLICY TO VENDORS/ SERVICE PROVIDERS:

Whenever any third party is signed for procuring software or database support care should be taken that there is no data leakage. The vendors should be given access to live databases. The vendors should not be allowed to make their presentations or demonstrations on the company terminals. All releases, patches and updates should be first verified in the test environment and then deployed in live.

XII. 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.________________.

XIII. 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