Risk Management Procedures

Company follows following policies with regard to Risk Management

A. Risk Management:

A sound risk management system is integral to an efficient clearing and settlement system. Clearing Corporation/Clearing House has put in place a comprehensive risk management system, which is constantly upgraded to pre-empt market failures. The Clearing Corporation ensures that trading member obligations are commensurate with their networth.

Risk containment measures include capital adequacy requirements of members, monitoring of member performance and track record, stringent margin requirements, position limits based on capital, online monitoring of member positions etc.

The Company follows prudent risk Management policies by collecting requisite margin money from Clients in selective cases which is decided based on track records of the clients, trading pattern etc and the decisions are taken on case to case basis. Terminals are provided based on the number of clients mapped to a single dealer. The Company has a dedicated team which monitors the debit balances on a daily basis. The Company does not have any long outstanding debts. The Company usually does not have outstanding debts older than 5-6 days. In very few cases, where the debts are outstanding for more than 5-6 days, the Relationship manager personally visits the client and ensures that the same is recovered. The Company does not charge any penal interest for long outstanding debts.

The Company follows the system of quarterly reconciliation wherein the client has expressly accepted the balance confirmation

The decisions about setting limits for the trades are decided by the Management and the same is not allowed to the Dealers to avoid any vested interest. The Company is maintaining proper accounts of all its clients so that no mistake will occur while effecting securities pay-in and pay-out and funds pay-in and pay-out.

Company never indulges in client funding as a measure of prudent risk management.

While effecting trades on behalf of Institutional Clients, Company follows the time schedule as prescribed by the Securities Regulations.

Company also takes care that it is not violating any of the provisions of applicable laws, rules or regulations.

B. Margin Trading:

Company does not indulge in to Margin Trading.

C. Exposure and Turnover:

Exposures are decided by the management for every client only after considering their previous trading habits, track record and financial status. These limits are reviewed periodically. The authority to set or change the limit for the clients lies with the management and not with the dealers to avoid any vested interest. The Company follows the policy of setting the turnover limit at Rupees Five Lakhs for every client on a single day.

D. Margin Collection

The company follows the policy of collecting the margin money from the clients based on their nature of trading and payment in form of cash/securities.

E. Pay-in of funds and securities

There is a system in place to ensure that there are no third party pay-in of funds and securities. A separate person has been designated to track the pay-in of funds and securities and who is constantly engaged in the follow-up regarding the same with the clients to ensure timely pay-in of funds and securities.

F. Offline Mode of Trades

Risk Management measures followed by the company pertaining to the offline mode of trades:

1. Trading Limits:

The Company considers the following factors before assigning the trading limits to its clients:

i. Financial Details
ii. Past trading habits of the clients
iii. Delay in payment for more than 4-5 days
iv. Instances of Cheque bouncing.

2. Third Party Funds or Securities:

The Risk Management Team follows an adequate system to ensure that the company does not accept third party funds or securities.

3. Real Time Basis:

There is adequate system in place through which Risk Management Team can check and keep track of the client position limits and mark to market (M to M) on real time basis.

4. **Message pop-up facility:**

If the client maintains a demat account in our In-house Depository Participant and if they inadvertently give an instruction to sell the shares not lying in their demat account with us, then a message is popped up on the screen of the dealer. It doesn't mean that the clients cannot trade in the shares maintained in the demat accounts of other depository participants. Also in case, the clients attempts to trade in excess of the exposure given to them, then a message is popped on the screen and the system restricts them to trade.

G. Online Trades or Internet Based Trading (IBT)

Risk Management measures followed by the company pertaining to the Online mode of trades:

Trading Limits:

There is a system in place to ensure that the Trading Limits assigned to the IBT clients are restricted to the funds transferred by the clients from their bank account. Clients can sell only those shares which are lying in their demat account maintained with our In-house depository participant.

Prohibition of trading in Z ,T, TS, BE, BT group of shares:

The company follows the policy of restricting IBT Clients from trading in the scrips of aforementioned groups. Special Permission is required from the risk management team to trade in the scrips of aforementioned groups.

Requirement for IBT Clients:

IBT Clients are mandatorily required to have the demat account with our In-house depository participant and bank account with any one of Axis Bank, HDFC Bank or ICICI Bank for availing Internet based trading facility.

NOTE: IBT HAS BEEN DISCONTINUED ON 31ST JANUARY,2012.

INTERNAL CONTROL POLICIES.

ACCESS TO DEALING ROOM.

Access to dealing room is restricted only to the dealers, IT engineers and to compliance officer. No one else is allowed to have access to the dealing room.

SOFTWARE SECURITY

Company is using licensed software for its operations. The original CDs of these Applications and Original License are kept under lock and key and only software engineers are allowed the access to them with the permission of IT Manager. All computers are protected with McAfee Antivirus or Microsoft Security Essential anti virus . Updation of this software is done online on periodic basis. Company has also installed Hardware Firewall from FortiGate. Configuring the firewall features is the responsibility of the IT staff. This software set up is considered to be sufficient, protecting the IT environment considering the size and operations of the Company.

The access to the back-office software is restricted to back-office staff and each individual is given access to the specific information required by him. The company has given full authority to “System Administrator account” used by IT Staff to create, modify, add or delete any functional rights of back-office.

HARDWARE SECURITY

Company is having proper facility and set up to protect its hardware from any damage. Hardware engineers are appointed to look after the hardware set up of the Company.
With regard to acquiring the hardware requirement. Company has empanelled the vendors which supplies genuine hardware to the Company.

Company has a policy of carrying out preliminary checks of the hardware acquired. At a later stage periodic checks are carried out by the IT engineers and in case of any problem, we have very efficient vendor support.

With regard to Power Failure we have UPS backup system in place. All the hardware and servers are located at a safe and secure place.

Users are not allowed to connect external devices like USB or any kind of Pen drives, mobile or any additional devices that can lead to data theft. As a security measure all USB ports are disabled and user willing to send data has to use company provided Pendrives only and all such data transfer should be done in presence of IT personnel

DOCUMENTATION POLICY AND INFORMATION STORAGE.

Critical Databases are backed up on daily basis and the same are transferred to remote PC on daily basis. Required Log files of CTCL server are also taken care off as per backup policy.

Backup of other data is taken regularly on monthly basis on removable media and stored at a different location.

Documentation is handled by the legal and Secretarial department of the Company and all the important documents are kept under the control and authority of the Company secretary.

PASSWORD POLICY

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of PPFAS's entire corporate network. As such, all PPFAS employees (including contractors and vendors with access to PPFS' systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any PPFAS facility,has access to the PPFAS network, or stores any non-public PPFAS information.

Passwords are used for logging on to System, ODIN Application in dealing room of PPFAS. Since ODIN Server forces password to be changed every 7 days, all dealers should be aware of how to select appropriate password required by ODIN Server.
ODIN Server requires :
Password length should be minimum 6 characters, maximum 12 characters & should be alpha-numeric.

All passwords are to be treated as sensitive, Confidential PPFAS information.
Here is a list of "dont's":
• Don't reveal a password over the phone to ANYONE
• Don't reveal a password in an email message
• Don't talk about a password in front of others
• Don't hint at the format of a password (e.g., "my family name")
• Don't reveal a password on questionnaires or security forms
• Don't share a password with family members
• Don't reveal a password to co-workers while on vacation

Change passwords immediately when prompted by ODIN Server.

If an account or password is suspected to have been compromised, report the incident to IT department and change all passwords.

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Please note that Odin is forcing password change every 15 days instead of 7 Days

RESTORATION AND ARCHIVAL POLICY

ODIN database is backed up on daily basis and the same is stored on off line server on weekly basis.

For Parag Parikh Financial Advisory Services Limited

Director