INTERNAL CONTROL

By

MSB e-Trade Securities Ltd.

Mem:

NSE/BSE/MSEI/MCX/NCDEX/ICEX/AMFI/DP:CDSL

Regd. & Corp. Office:-
C-603, Saraswati Vihar, Pitampura, Delhi-110034
☎ 011-47107777,
SEBI Single Registration no. INZ000184638

Exchange	Category	Member Id
NSE	Trading Member	12788
BSE	Trading Member	6395
MSEI	Trading Member	21000
MCX	Trading Member	29905
NCDEX	Trading Member	00732
ICEX	Trading Member	2062

&

AMFI REGN. NO. ARN – 78123
CDSL DP ID: 12070600 SEBI Regn. No. IN-DP-CDSL-261-2016
Repository Participant [RP] Id: 12070600

E-mail ID:-
info@msbetrade.com &
msbetrade@rediffmail.com

Exclusive E-mail ID for Investors Grievance:-
grievances@msbetrade.com
dpgrievances@msbetrade.com

Website: www.msbetrade.com

INTERNAL CONTROL POLICY

Index

1 - BRIEF OF INTERNAL CONTROL POLICY

INTERNAL CONTROL POLICY is requires for the purpose of controlling the activity of the organisation which is an important part of the organisation for their business enhancement & maintain the ethics for achieve the compliance level as per accordance with the rules, bylaw & regulation of the regulatory.

Internal control is the integrated of the activities, plans, attitudes, policies, applicable laws and regulations, and efforts of the people of an organisation working together to provide reasonable assurance that the organisation will achieve its objective and mission.

2 - INFORMATION SECURITY

PURPOSE

By information security we mean protection of the Organisation's data, applications, networks, and computer systems from unauthorized access, alteration, or destruction.

The purpose of the information security policy is:

- To establish a Organisation-wide approach to information security.
- To prescribe mechanisms that help identify and prevent the compromise of information security and the misuse of Organisation data, applications, networks and computer systems.
- Confidentiality of information:
- E-mail should not be used for confidential information exchange
- Clients/ Employee Information maintain & keep in safe custody of the company after the proper verification.

Appropriate Use

- The computers of the Organisation are used only by the relevant authorised persons only by their relevant password only.
- The Authority of accessing of back office Software (i.e. shilpi) where all the data related to Clients has been controlled by the user ids & their relevant passwords.
- The Authority for working on back office software (i.e. shilpi) has been distributed according to the nature of their work.
- The Documents related to the Organisations & their clients are maintained by the appointed persons only under the supervision of the senior official of the organization. No other persons are permitted for access the documents without the permission.
- Sharing of information related to the organizations & their clients prohibited sharing with the outsider of this organization.
- Use of e-mails will be restricted for business use only.

3 - PRIVACY POLICY

This privacy policy sets out how **"MSB e-Trade Securities Ltd."** uses and protects any information that you give **"MSB e-Trade Securities Ltd."** when you use this website.

"MSB e-Trade Securities Ltd." is committed to ensuring that your privacy is protected. Should we ask you to provide certain information by which you can be identified when using this website, then you can be assured that it will only be used in accordance with this privacy statement.

"MSB e-Trade Securities Ltd." may change this policy from time to time by updating this page. You should check this page from time to time to ensure that you are happy with any changes.

What we collect

We may collect the following information:

- name and job title
- contact information including email address
- demographic information such as postcode, preferences and interests
- other information relevant to customer surveys and/or offers

What we do with the information we gather

We require this information to understand your needs and provide you with a better service, and in particular for the following reasons:

- Internal record keeping.
- We may use the information to improve our products and services.
- We may periodically send promotional email about new products, special offers or other information which we think you may find interesting using the email address which you have provided.
- From time to time, we may also use your information to contact you for market research purposes. We may contact you by email, phone, fax or mail.
- We may use the information to customize the website according to your interests.

Security

We are committed to ensuring that your information is secure. In order to prevent unauthorized access or disclosure we have put in place suitable physical, electronic and managerial procedures to safeguard and secure the information we collect online.

How we use cookies

A cookie is a small file which asks permission to be placed on your computer's hard drive. Once you agree, the file is added and the cookie helps analyse web traffic or lets you know when you visit a particular site. Cookies allow web applications to respond to you as an individual. The web application

can tailor its operations to your needs, likes and dislikes by gathering and remembering information about your preferences.

We use traffic log cookies to identify which pages are being used. This helps us analyse data about web page traffic and improve our website in order to tailor it to customer needs. We only use this information for statistical analysis purposes and then the data is removed from the system.

Overall, cookies help us provide you with a better website, by enabling us to monitor which pages you find useful and which you do not. A cookie in no way gives us access to your computer or any information about you, other than the data you choose to share with us.

You can choose to accept or decline cookies. Most web browsers automatically accept cookies, but you can usually modify your browser setting to decline cookies if you prefer. This may prevent you from taking full advantage of the website.

Links to other websites

Our website may contain links to enable you to visit other websites of interest easily. However, once you have used these links to leave our site, you should note that we do not have any control over that other website. Therefore, we cannot be responsible for the protection and privacy of any information which you provide whilst visiting such sites and such sites are not governed by this privacy statement. You should exercise caution and look at the privacy statement applicable to the website in question.

Controlling your personal information

You may choose to restrict the collection or use of your personal information in the following ways:

- whenever you are asked to fill in a form on the website, look for the box that you can click to indicate that you do not want the information to be used by anybody for direct marketing purposes
- if you have previously agreed to us using your personal information for direct marketing purposes, you may change your mind at any time by writing to or emailing us at [email address]

We will not sell, distribute or lease your personal information to third parties unless we have your permission or are required by law to do so. We may use your personal information to send you promotional information about third parties which we think you may find interesting if you tell us that you wish this to happen.

You may request details of personal information which we hold about you under the Data Protection Act 1998. A small fee will be payable. If you would like a copy of the information held on you please write to [address].

If you believe that any information we are holding on you is incorrect or incomplete, please write to or email us as soon as possible, at the above address. We will promptly correct any information found to be incorrect.

RECORD KEEPING

- All the Documents with the relevant to the conduct of the business of the company to be keep under the safe custody of the person designated to do such act.
- Client's information is the valuable for the company growth. That's why all the record with the client registration document under the safe custody of the person appointed to do such act.
- All the documents with relevant to the company & Clients registration documents are strictly restricted to retrieval other than person or persons appointed to do such act.
- All the information of the client also restricted to share with other than person related to the company.
- All the information & documents with related to client registration documents & other documents provide to respective client only after the requesting by such client or provide to the authorities as per the rule, bylaw & regulations of the exchanges, regulatory and other authorities which is authorised to get such information.

4 - Backup

Backup Policy

Overview
This policy defines the backup policy for computers within the organization (onsite on-line backup) & off-site off-line backup which are expected to have their data backed up.

Purpose
This policy is designed to protect data in the organization to be sure it is not lost and can be recovered in the event of an equipment failure, intentional destruction of data, or disaster.

Scope
This policy applies to all equipment and data owned and operated by the organization.

Timing
The Organization must take Full backups performed nightly on daily (every working day) basis at user level as well as admin level.

Storage of Back up

The Organization is taking onsite on-line backup on the server itself on daily basis, off-site off-line backup on Two USB drive/CD media/dat drive (80 GB) on daily/weekly basis. One USB drive/CD media/dat drive is kept at the office area another at the remote site.

Testing of USB drive / CD media

The Organization is testing periodically USB drive / CD media/ DAT drive, which are used for storage of off-site off-line backup backup. If there is any possibility for change / replace of such storage media then get it done by the responsible person of the organization.

Responsibility
The Organization appointed a persons perform regular backups. The appointed person must follow develop a procedure for testing backups and test the ability to restore data from backups on a daily/weekly basis.

Testing
The ability to restore data from backups shall be tested by senior official of the organization.

Backup Register

The Organization is maintaining the backup registered (Physically or electronically) for the purpose of maintain the records for daily backup taken by whose official and when it taken.

This policy defines the backup policy for computers within the organization (onsite on-line backup) & off-site off-line backup which are expected to have their data backed up.

The Organization must take Full backups performed nightly on daily (every working day) basis at user level as well as admin level.

The Organization is taking onsite on-line backup on the server itself on daily basis, off-site off-line backup on USB drive/CD media on daily/weekly basis. USB drive/CD media is kept at remote site.

The Organization adequate Backup facility as we have two dat drive (One is 500 GB other one is 500 GB sure store DAT) in which we take backup of all of our important data.

The Organization appointed a persons perform regular backups. The appointed person must follow develop a procedure for testing backups and test the ability to restore data from backups on a daily basis.

The ability to restore data from backups shall be tested by senior official of the organization.

5 - Password Policy

Overview

Passwords are an important aspect of computer security. They are the front line of protection for user IDs/accounts. A poorly chosen password may result in the compromise of entire corporate network. As such, all employees are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Purpose

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.

Scope

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 facility, has access to the network, or stores any non-public information.

Policy

(A) General

- All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a monthly basis.
- All user-level passwords (e.g., user ids, etc.) must be changed at least every15 days.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- All user-level and system-level passwords must conform to the guidelines described below.

(B) Guidelines

Password Creation Guidelines:

The following password creation guidelines are based upon experience and common sense. The software used to change passwords will screen for most of these guidelines as an aid in creating secure passwords. This does not relieve a person of responsibility for creating and securing a good password.

- It must be at least eight characters in length. (Longer is generally better.)
- It must contain at least one alphabetic and one numeric character. (Alpha – Numeric generally better)
- It must be significantly different from previous passwords.
- It should not be the same as the user ID, email IDs, telephone no., date of birth, nick name, house no., vehicle no., & some common nos.
- It should not start or end with the initials of the person issued the user ID.
- It should not include the first, middle, or last name of the person issued the user ID.
- Special characters may be used to strengthen the password.
- It should not be information easily obtainable about you. This includes license plate, social security, telephone numbers, or street address.

(C) General Password Construction Guidelines

Passwords are used for various purposes at **MSB e Trade Securities Ltd.** Some of the more common uses include:

User level, accounts, email, screens saver protection. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
  - Names of family, pets, friends, co-workers, fantasy characters, etc.
  - Computer terms and names, commands, sites, companies, hardware, software.
  - The words "<MSB e_TRADE SECURITIES LTD.>
  - Birthdays and other personal information such as addresses and phone numbers.
  - Word or number patterns like aaabbb, qwerty, zyxwvuts, , aaaaaaaa, 123321, 123456, 00000000, etc.

Any of the above spelled backwards.

Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

NOTE: Do not use either of these examples as passwords!

(D) Password Protection Standards

- Do not share < MSB e_Trade Securities Limited > passwords with anyone, including administrative assistants or secretaries.
- All passwords are to be treated as sensitive, Confidential < MSB e_Trade Securities Limited > 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 reveal a password to the boss
- 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
- If someone demands a password, refer them to this document or have them call Direct to the Director without hesitation.
- Do not use the "Remember Password" feature of applications.

- ☞ Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.
- ☞ Change passwords at least once every 15 days. The recommended change interval is every 15 days.

If password is suspected to have been compromised, report the director and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by InfoSec or its delegates.

If a password is guessed or cracked during one of these scans, the user will be required to change it.

6 - Risk Management System (RMS)/ Surveillance PROCESS

The purpose of RMS Policy is eliminating the risk of the Company /client from the volatility of the market.

6.1 RMS works on the following concepts:

a. **Cash**

The clear balance available in the customer's ledger account in our books.

b. **Margin**

The underlying stake provided by the customer in the form of cash, FDR and/or stock to mitigate market (price) or settlement (auction) risk

c. **Exposure**

The aggregate of the customer's obligations arising out of buy + sell trades awaiting settlement in the cash segment and profit/ loss amounts that are yet to be settled on the closed positions.

d. **Exposure multiple**

The number of times that exposure is allowed on the underlying margin sales on the cash segment would have to be made either on the availability of cash margin or on the availability of the stocks (which are to be sold) in our margin account, by executing a transfer before the sale order is initiated.

e. **Stock qualifying for margin in cash & F&O segment transactions**

Securities in the approved list of Stock Exchange as per SEBI guidelines after applicable hair cut as per exchange.

d. **Total Deposit**

The aggregate of client deposit available with us in the form of cash, Shares (After Applicable Hair Cut) and FDR.

e. **Mark to Market Losses**

Mark to market losses shall be collected in the following manner:

- Mark to market loss shall be calculated by marking each transaction in security to the closing price of the security at the end of trading. In case the security has not been traded on a particular day, the latest available closing price at the exchange shall be considered as the closing price. In case the net outstanding position in any security is nil, the difference between the buy and sell values shall be considered as notional loss for the purpose of calculating the mark to market margin payable.
- The mark to market margin (MTM) shall be collected from the member before the start of the trading of the next day.
- The MTM margin shall also be collected/adjusted from/against the cash/cash equivalent component.
- The MTM margin shall be collected on the gross open position of the Client.

- There would be no netting off of the positions and setoff against MTM profits across two rolling settlements i.e. T day and T-1 day. However, for computation of MTM profits/losses for the day, netting or setoff against MTM profits would be permitted.
- In case of Trade for Trade Segment (TFT segment) each trade shall be marked to market based on the closing price of that security.
- The MTM margin so collected shall be released on completion of pay-in of the settlement.

6.2 CATAGORY OF CUSTOMER TRANSACTIONS

a. **Intraday - Cash segment**

The amounts of purchase (or sale) in a scrip on any trading day that is reversed by the end of the day by making a contra sale (or purchase) of the exact same quantity, thereby nullifying the original position.

b. **Delivery Trades**

The net purchase or sale of scrip in a client account that is settled by way of a delivery on T+2. Delivery in respect of sale transactions in the cash segment has to be settled by the client by tendering securities in demat form before the pay-in deadline. Else the client faces the risk of auction. A purchase transaction in the cash segment would fall into one or more of the following categories:

c. **Sell against Buying**

A purchase order executed on the Exchange today and the (undelivered) purchased stock sold in its entirety on the next trading day. In this case the first transaction would be settled on T+2 while the sale would be settled on the third business day after the purchase transaction.

e. Execution of Orders – For Execution of orders define the limit as under as per the USER ID & BRANCH ID basis :-

- Quantity limit for each order.
- Value Limit for each order.
- User value limit for each user ID.
- Branch value limit for each branch ID.
- Security wise limit for each user ID.

6.3 Handling of client Securities

(A) The following demat account to deal with the client securities:-

i. Pool account (MSB e-Trade – Pool account)
ii. Client Unpaid Securities Account
iii. Early Payi-in Account
iv. Client collateral Account (for holding client securities for margin purpose and onward transfer to Collateral Account for pledging with Clearing Corporation ("CC") or transfer to Clearing Member ("CM")
v. Collateral Account (for pleading own & Client securities with CCs)

(B) As per normal practise to deal with the securities of the client which the client bought through their trading a/c or transfer to us, we used to transfer these securities of the client into their registered demat account except in the following circumstances:

(i) "***Unpaid Securities***" (for which the client(s) not paid or partially paid) – In case of non-payment or partial payment, Securities are kept in "***Client Unpaid Securities Account***" (partial or fully) & shall be disposed-off (partially or fully based on their unpaid amount) with 5 days from the pay-out or;

Based on earlier record of the Client with us we Can be return to the client's there unpaid securities (partially or fully) in case client given us the Power of Attorney "POA" to meet the client obligation in their registered demat account maintained with MSB e-Trade (DP-CDSL).

(ii) "***Client Collateral Account***" This Demat A/c for the purpose of holding client securities for margin purpose or for transferring to Clearing Members. Such securities shall be transferred to the "Collateral Account" for pledging with the clearing corporation and

(iii) For transferring to Clearing corporation – for this purpose securities are kept in "***Collateral Account***" (for pledging own & Client securities with CCs)

(C) In case there are multiple securities in the "Client unpaid securities account" and the Stock Broker wishes to liquidate the same, is there any logic like First in First Out (FIFO) to be followed?

If there are multiple securities in the "Client unpaid securities account" then MSB e-Trade may take following steps/ decision

1. Based on the unpaid amount of the securities we will try our level best to liquidate the higher price securities after comparing the previous close price at the time of liquidate the unpaid securities.
2. The time of liquidation can be any time on day of liquidation.
3. If there are no major difference in the price of the multiple securities then any of the securities can be liquidate or FIFO method to be followed.

DO: (also please refer above and exchange's circulars for details)

- ✓ Client Securities kept in "Client Unpaid Securities Account" only be transferred to Respective client Demat A/c or to Pool A/c. (the quantify of securities based on the payment i.e. fully or partially)
- ✓ Securities can be transferred from "Client Collateral Account" or "Collateral Account" to Pool account for the purpose of making pay-in for settlement of respective client.
- ✓ Client Securities can receive in the "Client Collateral Account" and can be transferred to Clearing Member or "Collateral Account" for pledging with CCs.
- ✓ However, sale of securities lying in collateral account, based on client's instruction, can be considered towards such unpaid securities provided clear funds are received within such 5 trading day.
- ✓ Based on earlier record of the Client with us we Can be return to the client's there unpaid securities (partially or fully) in case client given us the Power of Attorney "POA" to meet the client obligation in their registered Demat account maintained with MSB e-Trade (DP-CDSL).

DON'TS: (also please refer above and exchange's circulars for details)

- × Securities cannot be transferred from "Client unpaid securities account" directly to the "Client Collateral account" or "Collateral Account"
- × Client Securities cannot be transferred from "Client Collateral Account" or Collateral Account to "Client unpaid securities account"
- × Securities kept in "Client unpaid securities account" cannot be considered towards client's margin obligation.
- × Further exposure cannot be grant to such client having debit balances.

6.4. Offline Alert / Back Office Alert

We are further investigated at the time of generation of billing by the Back Office Billing Department & the scrips are scanned for the quantity traded vis-a-vis exchange volume on that day, the frequency of trade done by the client & see if a trend is discernible.

The surveillance clientwise takes cue from the alerts generated scripwise. All the clients who have traded in the scrip placed in "SCRIP ALERT" are scrutinized for their other scrip dealings. Looking at the general quality of scrips that they are dealing in, Surveillance Officer reports to the Director for further action.

Further any big value transactions are checked for whether the client is not trading beyond ones known Income (i.e. Income declared in KYC)

Note – MSB e-Trade will not be responsible for any Short payout of security from exchange.

7 MARGIN COLLECTION AND REPORTING PROCEDURE

MARGIN REPORTING/ INFORMATION TO CONSTITUENTS

Client Margin information will convey to according to the following procedures:

First of all the information convey to client by telephonically or by email (which ever is applicable) to the relevant client on same day (trading day) basis about their margins & positions in Future & Options Segment by the back office department (F&O).

Secondly the Printed Document for information regarding the margin information is sent to the client as per exchange by Hand or By Courier to the client. The information is in printing form from the back office software having the following details about their margins in future & options :-

Total Deposit for the Day T-1 (T=Trading Day)
Margin Utilised for the Day T-1 (T=Trading Day)
Margin Deposited for the Day T (T=Trading Day)
Margin Utilised for the Day T (T=Trading Day)
Margin status end of day T (T=Trading Day)
Running Balance
Days MTM

Client Margin information also clarify to the relevant client if required the all the necessary details must be provided to clients

MARGIN COLLECTION FROM CONSTITUENTS

After the information given by telephonically and in printed form to the relevant client about their Margin then the required margin will be asked from the relevant client within the period as prescribed by the exchange.

The required margin will collect from the constituents before with the time period as prescribed by the exchange from time to time by cheque /demand draft only at the earliest.

Note : This procedure follow by the M/s MSB e-Trade Securities Ltd. it will review time to time and put the necessary modification.

8 Capacity Management

Capacity Management ensures that adequate capacity is available to deliver the services such that the Service Levels are not compromised due to resource crunch. It is a day to day operation like the Service Support functions but has been placed under Service Delivery because strategic inputs from the other Service Delivery functions are very important for its accuracy and delivery efficiency.

Capacity Management can classified into two types: Service Capacity Management and Resource Capacity Management.

Service Capacity Management: This is driven by the current service trends, target Service Levels defined by Service Level Management and/or Business inputs from the management. In this category the Capacity Management Function would focus on adequate skilled manpower, availability of vendors, availability of space (example, seating and storage areas), capacity of Communications facilities (like telephone lines), etc.

Resource Capacity Management: This is driven by the capacity of the current technology infrastructure, the future scalability, and the capacity burn rate.

These two Capacity Management areas can have common work areas. However the focus of the former is to maintain targeted Service Levels and focus of the latter is to maintain targeted Technology Levels. To deliver the services accurately, both of them need timely and accurate inputs from:

The Management - Pertaining to future business expansions or acquisitions, Budgets, financial growth plans, etc.

- The Service Level Management - Pertaining to target service levels.
- Change Management - Pertaining to Forward Planning with schedules and Magnitudes of Changes.
- The System Monitoring - Pertaining to Transaction Volume Trend Analysis, Capacity Burn Rates, Performance Trends, etc - all with accurate triggers and alerts at the right time.

The Organization review there capacity regarding the Service & Resource after some time or when necessary like:-

- ☞ Monitoring of performance and throughput of all services
- ☞ Deploying new technology in line with business requirements (time, cost, and functionality).
- ☞ All networking equipment: LANs, WANs, bridges, routers, and so on.
- ☞ All Hardware: Hard Disk, Ram, Mouse, Key Board, Printer etc.
- ☞ All peripherals: Storage devices, printers, and so on.
- ☞ All software: Operating system, network, in-house developed, and purchased packages,

9 NETWORK SECURITY POLICY

Preamble

This document establishes the network security policy for the M/s MSB e-Trade Securities Ltd, MSB e-Trade, MSB.

The network security policy is intended to protect the integrity of MSB networks and to mitigate the risks and losses associated with security threats to MSB networks and network resources.

Goals

The goals of this network security policy are:

- to establish Corporate wide policies to protect the MSB e-Trade's networks and computer systems from abuse and inappropriate use.
- to establish mechanisms that will aid in the identification and prevention of abuse of MSB e-Trade networks and computer systems.
- to provide an effective mechanism for responding to external complaints and queries about real or perceived abuses of MSB e-Trade networks and computer systems.
- to establish mechanisms that will protect the reputation of the MSB e-Trade and will allow the MSB e-Trade to satisfy its all responsibilities with regard to its networks' and computer systems' connectivity to the

Policy Statement

The MSB e-Trade provides network resources to its organizations in support of its Trading Activity. This policy puts in place measures to prevent or at least minimize the number of security incidents on the organisations network without impacting the Trading Activity or the integrity of the MSB e-Trade's many different computing communities.

The responsibility for the security of the MSB e-Trade's computing resources rests with the system administrators who manage those resources. Technical Operations persons will help to carry out these responsibilities according to this policy.

The **Technical Operations persons** of the organisation will review and respond to formal complaints resulting from the implementation of this policy.

Technical Operations persons which administer LANs connected to the backbone will:

- assign to an individual, the authority to connect systems to the organisation network(s).
- ensure this information is kept accurate and up to date.

The Computer Security Technical Operations Persons will:

- co-ordinate all CNS network security efforts and act as the primary administrative contact for all related activities,

- co-ordinate investigations into any alleged computer or network security compromises, incidents and/or problems.
- co-operate in the identification and prosecution of activities contrary to MSB e-Trade policies. Actions will be taken in accordance with relevant MSB e-Trade Policies, Codes and Procedures with, as appropriate, the involvement of the Campus Police and/or other law enforcement agencies,
- in consultation with system administrators, develop procedures for handling and tracking a suspected intrusion, and deploy those procedures in the resolution of security incidents.
- Ensure that no one can access to the other network.

Technical Persons will:

- protect the networks and systems for which they are responsible,
- employ CNS recommended practice and guidelines where appropriate and practical,
- co-operate with CNS in addressing security problems identified by network monitoring,
- address security vulnerabilities identified by CNS scans deemed to be a significant risk to others,
- report significant computer security compromises to Computer Security Administration.

Network users will:

- abide by the Appropriate Use of Information Technology policy of the MSB e-Trade,
- abide by this policies governing connection to organisation networks.

10 Application Software Policy

1. Introduction The availability, reliability and integrity of a Use & developed application system, is a critical service provided by Services Providers like FT, Shilpi & Microsoft etc & also the software provided by the exchange.

Development of Application Software

These developed applications come about when there is a requirement to meet Organization needs.

The objective of this policy is to create an environment for the meaningful and consistent application development to attain high quality results.

Definition

Application software development is the act of reviewing, evaluating, designing, coding (programming) and implementing a software application by Service Providers through the technical department time to time.

Development of Application software is done by the software vendors under the needs of organization through the technical department time to time.

Some of the software update under the instructions of the NSE or service providers on regular basis.

Conditions of Use

Only authorised persons has right to access the application software those are use by the organization.

Every users has different authority according to the nature of there work i.e accounts persons has the different authority rather than the person look after the DP or trading software.

Instructions to the Users of the application software for an organization.

1. Almost the application software has there login ids & password.
2. Users are instructed not to share there password of the application software.
3. The Password must be alpha numeric & must be changed periodically
4. Users are clearly prohibited for access user of others. Prior intimation & permission is required for use of different user.
5. Where is the concern of “TRADING TERMINALS” All the orders are accepted by the clients after authentication of identity of the client like ‘Code’ / ‘Pan No.’/ ‘DOB’ etc. & then punch to trading terminals.

11 Business Continuity Planning and Disaster Recovery

Business continuity planning and disaster recovery planning are fundamental to the well being of an organization. Clearly, they are intended to ensure continuity in the face of unforeseen or difficult circumstances.

Planning for these situations is not always straight forward of course, and neither is identifying suitable sources of information, services and products. The requisite planning tasks themselves can also be challenging.... none more so than the building of the plan itself.

Introduction

With the increasing importance of information technology for the continuation of business critical functions, combined with a transition to an around-the-clock economy, the importance of protecting an organization's data and IT infrastructure in the event of a disruptive situation has become an increasing and more visible business priority in recent years.

Our business is based on technology like Computer VSAT, Lease line, router, Internet services & telephone etc.

"We can say that if business is the life than the technology is the heart"

Level 1:.Minor Outage Scenario

In the event of a minor outage, business processes may experience minor damage / outage and will run at a sub-standard level. Scenarios include link connectivity being temporarily down, switch or router port failures, System or network CPU failures, System Fan failures, System or Network Power supply failures, Ethernet card failures.

PLAN:

Company deputes the Technical person for technical problem like switch, router port failures system failures, Ethernet card failures for rectification at the earliest or replacement. Company keeps all necessary equipment in spare for replacement.

Level 2: Moderate Outage Scenario

In this scenario, some or all business processes at the location may experience moderate damage / outage. Processes may not continue or may run at a degraded level. An alternate site may not be required for continuing business but alternate equipment may be required depending on the criticality of the business process and infrastructure.

Some of the examples of such scenarios can be:-

1. Equipment is damaged due to Power surge.
2. ISDN/VSAT/Circuit router failure
3. Core access layer switch failure
4. Access/Distribution switch failure.
5. LAN switch or router failure.
6. Temporary outage of power.

PLAN :

Company is having 1 (One) VSAT (Very Small Aperture Terminal) & 1 (One Lease line) with auto transfer scenario from Lease line to VSAT & vise-a-versa.
In case of damaged of any equipment technical person replace at the earliest.

Company is having UPS as a backup for temporary power supply, which is automatically works after power failures, also having a Generator for power supply.

Level 3: Disaster Scenario

In this scenario, the Member infrastructure may experience a severe disaster resulting in the total shut down of infrastructure of the Member. Full processing capability of all business processes like Trading, Risk Management, settlement systems etc. from that location and related infrastructure may be down. Key personnel may not be able to access the premises. There may also be non-availability of key resources in the building.

Some of the examples of such scenarios can be
1. Flood / Rain/Fire making office premises like building and Data centers inaccessible.
2. Riots /war etc., at a location near one of the offices or within the premises of the member may render the office premises inaccessible.
3. Complete power shutdown due to unavailability of generators.

In this scenario if complete power shutdown due to unavailability of generators we are also having UPS for power supply.

We are having our branch, where our business can be carried out due to any shutdown in the main office.

Under this scenario, Members may have to switch their business over to the BCP site. Key factors which will determine the Recovery Time Objective would be key personnel availability, resilient IT infrastructure and robust BCP processes.

Level 4: Catastrophe

In this scenario, a major disaster strikes which would result in a major disruption of services. Full processing capability cannot be achieved for a substantial period of time. Recovery will require use of alternate processing site as well as offsite offices for employees over an extended period of time
Some of the examples of such scenarios can be

1. War
2. Earthquake
3. Extended Communal Riots etc

In such a scenario, capability to achieve their Recovery time objectives would critically depend upon Key personnel availability, resilient IT infrastructure and robust BCP processes.

PLAN:

Company is having the internet connectivity of the exchange for this purpose every client of the company can do the trade direct with exchange provided platform along-with their provide login id & password.

12 POLICY REGARDING TREATMENT OF INACTIVE ACCOUNTS

M/s MSB E-TRADE SECURITIES LIMITED as a matter of policy accepts and realizes that the investor community is made of traders as well as investors. Whereas traders trade frequently, the investors trade with long gaps. The inactive client policy is framed keeping the same in mind:

What happens when a client is declared inactive?

On a client being declared inactive,

1 All the securities of the client are transferred into the last known demat account of the client.
2 All the funds of the client are returned to the client.
3 In case the demat account/ bank account details are not available or/and the client is not contactable, the securities/ funds are transferred into a separate account of MSB e-Trade and held till such time MSB e-Trade hears from the client or their representatives.
4 Trading in the client account is stopped.

Client declared inactive voluntarily
A client may write to MSB e-Trade stating that he wishes to transfer his account into an "inactive" status, based on which the account will be marked as such.

Client declared inactive by passage of time
Any client who has not traded even a single trade for a period of 1 years will be considered as inactive and will automatically be moved to the "inactive" category.

Client declared inactive by law
Any client will be moved to the "inactive" category if required by law.

Procedure to activate the client
To reactivate the account, the client is expected to write to the TM requesting for activation of the account, based on which the account would be activated after due diligence by the TM.

13. POLICY FOR CONDUCT FOR PREVENTION OF INSIDER TRADING

The purpose of this Policy is to maintaining code of Internal Procedures and Conduct for prevention of Insider Trading.

The organization/firm has a senior level employee reporting to the Managing Partner/Chief Executive Officer.

The senior level employee shall be responsible for setting forth policies and procedures and monitoring adherence to the rules for the preservation of "Price Sensitive Information", pre-clearing of all designated employees and their dependents trades (directly or through respective department heads as decided by the organization/firm), monitoring of trades and the implementation of the code of conduct under the overall supervision of the partners/proprietors.

The senior level employee shall also assist all the employees/directors/partners in addressing any clarifications regarding SEBI (Prohibition of Insider Trading) Regulations, 1992 and the organization/firm's code of conduct.
The senior level employee shall maintain a record of the designated employees and any changes made in the list of designated employees.

Preservation of "Price Sensitive Information"
Employees/directors/partners shall maintain the confidentiality of all Price Sensitive Information. Employees/directors/partners must not pass on such information directly or indirectly by way of making a recommendation for the purchase 55[or] sale of securities.

Prevention of misuse of Price Sensitive Information
Employees/directors/partners shall not use Price Sensitive Information to buy or sell securities of any sort, whether for their own account, their relative's account, organization/firm's account or a client's account. The following trading restrictions shall apply for trading in securities.

Pre-clearance of trades
All directors/officers/designated employees of the organization/firm who intend to deal in the securities of the client company (above a minimum threshold limit to be determined by the organization/firm) shall pre-clear the transactions as per the predealing procedure as described hereunder.

14. POLICY FOR UNAUTHENTIC NEWS CIRCULATION

- No staff member or associate is authorised to send any communication to any client by way of SMS / Email / Letter / Notice / etc., unless such communication is specifically authorised by the Compliance Office
- Any Equity Research Reports, Advisory Notes and Stock Recommendations sent out to the client can be sent out only from a designated Sender ID and should be duly authorised by the Compliance Officer.
- Log of all such communication sent to the clients should be maintained.

15. WRITE UP ON REDRESSAL FOR INVESTOR GRIEVANCE REDRESSAL POLICY

- ❑ The designated Email ID for lodging investor complains should be clearly displayed on the website and on all information sent to the clients
- ❑ An investor grievances escalation matrix should be clearly displayed on the website of the company
- ❑ All the investor complaints received by email on the designated email ID should be duly saved and recorded in the investor grievances register.
- ❑ All investor grievances which are not redressed at the first level must be escalated to the next level within 7 days
- ❑ Information regarding SEBI complaint redress system (SCORES) regarding filing of complaint on SCORES – Easy & Quick provide on website of the company.
- ❑ And the director link for SCORES provide on the website of the company.

16. Client Code Modification "CCM" and error Code Policy

Client Code Modification (Rectification of error code) "CCM" is a vital problem of the broking company. The main objective of a policy for Client code modification or Rectification of error code for post trade execution and takes the report on such modification/rectification of client codes. Also aware the dealers/trading personals about the policy for Client Code Modification (Rectification of error code) "CCM".

A. Circumstances about Client code Modification

"CCM" means modification of client code of those order has been executed or those order has converted to become trade. The stock exchange provides a facility to modify the client code to rectify an error. Further only the genuine errors will be modify and after being transferred to 'Error Account'. The modification should be done within the Stock Exchange guidelines. The modification of client code is to be done only in exceptional cases and not in routine case.

B. Details about Genuine error

The following trades shall be modify/ allowed to be modify, shall be treated as genuine error and transferred to Error Account.

- ✓ Punching error / typing error of client codes due to any genuine error or mistake in order entry, while punching the order, by any of dealer.
- ✓ Trade entered for wrong client due to any miscommunication from the client /authorized representative of the client.
- ✓ Client code/name and modified client code/name are similar to each other but such Modifications are not repetitive.
- ✓ Family Code (spouse, dependent parents, dependent children and HUF)
- ✓ Institutional trades modified to broker error/pro account.

C Classification of Genuine Error

The criteria for determining the genuineness of client code modification are as follows:

- ✓ Client code M020 wrongly entered N020 (if there is punching error), whereas M020 entered as M002 or M200 may be a genuine punching error.

D. The Board and Management Directives

The Board and Management of the company have approved under mention policy in this regard and instruct all the staff of the office to follow it strictly.

- ✓ It has been decided that a separate error account in the name of "**MSB e-Trade Securities Limited"** must open as per the exchange circular for rectification.
- ✓ It has been decided that client code mapping in trading terminals to prevent the punching error into those codes which are not given to anyone.
- ✓ It has been decided to periodically review the list of inactive clients into CTCL System.
- ✓ It has been instruct to all the Dealers to hear clearly the client code /scrip name /price and reconfirm the same before placing order into the trading system.
- ✓ /management on the implementation of the said policy periodically.
- ✓ It has been decided that maintain the register for "CCM" with immediate effect for recording the errors.
- ✓ It has been advice to the Department head/ Compliance officer for analyses the mistake and to take/implement corrective measures to their best possible efforts to minimize the same.

- ✓ It has been advice to the Department Head/ Compliance officer to update the Board regarding the same.

E Reporting System

- ✓ Any issues regarding the "CCM" should be reported to the designated officer and can be done only after getting approval after knowing it's genuinely as per exchange directives.
- ✓ Any client code modification shall be subjected to this policy be carried at Head Office of the company in the normal circumstances.
- ✓ The designated officer review the Error Account file send by the Exchange on daily basis.
- ✓ A separate register for "CCM" to be maintained by the company for above purpose where full details will be recorded.

F Reference to the Circular

F (i) SEBI – Circulars No. – CIR/DNPD/6/2011 dated January 01, 2011
Circulars No. – CIR/DNPD/01/2011 dated July 05, 2011

F(ii) NSE – Circular No. - NSE/INVG/2011/596 dated February 17, 2011
Circular No.- NSE/INVG/2011/18484 dated July 29, 2011
Circular No. - NSE /INVG/2011/870 dated August 26, 2011.

17 Policy for PRE FUNDED INSTRUMENTS from Clients

Objective:
The objective of the policy is to prevent acceptance of third party funds and to prescribe process to deal with instruments issued by third party when received.

Background:
SEBI vide circular no. SEBI/MRD/SE/Cir-33/2003/27/08 dated August 27, 2003 has specified that the stock brokers can accept demand drafts from their clients. However, SEBI vide circular no. CIR/MIRSD/03/2011 dated June 9, 2011 and National Stock Exchange vide its circular no. NSE/INSP/18024 dated 09-Jun-11 has advised stock brokers to maintain an audit trail while receiving funds from the clients through Demand Draft (DD)/Pay Order (PO)/Bankers Cheque (BC) since such third party pre-paid instruments do not contain the details like name of the client, bank account number are not mentioned on such instruments. Non maintenance of audit trail may result in flow of third party funds or unidentified money which may result into breach of regulations issued under PMLA and SEBI circulars.

Terms used in this policy:
1. **Prefunded Instruments** - Referred as Payorder, Demand Draft, banker's cheque etc.
2. **Electronic Fund Transfers -** Referred as transfer of funds using net banking

Policy:
SEBI vide circular no. SEBI/MRD/SE/Cir-33/2003/27/08 dated August 27, 2003 has specified that the stock brokers can accept demand drafts from their clients. However, in accordance with SEBI circular no. CIR/MIRSD/03/2011 dated June 9, 2011, the following needs to be complied:

1. A "Pre-paid instrument received register" with columns for date, name of the client, Particulars of instrument (like amount, instrument drawn on bank name) and such other columns as found necessary shall be maintained. The register may be maintained either in a physical form or in electronic form.
2. Pre-paid instruments of the value of less than Rs 50,000 may be accepted from the client. Whenever such instruments are received, entry into 'Pre-paid instruments Received register' shall be made.
3. If the pre-paid instrument is for value more than Rs 50,000 or If the aggregate value of prefunded instruments is Rs. 50,000/- or more, per day per client is presented for acceptance, such instrument or instruments may be accepted, only if the same is/are accompanied by the name of the bank account holder and number of the bank account debited for the purpose, duly certified by the issuing bank. The mode of certification may include the following:
    a. Certificate from the issuing bank or its letter head or on a plain paper with the seal of the issuing bank.
    b. Certified copy of the requisition slip (portion which is retained by the bank) to issue the instrument.
    c. Certified copy of the passbook / bank statement for the account debited to issue the instrument.
    d. Authentication of the bank account-number debited and name of the account holder by the issuing bank on the reverse of the instrument.

4. If a client submits pre-paid instruments at different times during the day, details and certificates as stated above may be collected along with the instrument with which the aggregate value of pre-paid instruments submitted exceeds Rs 50,000 for that date.
5. In case of any receipt of funds by way of Electronic fund transfer, an audit trail to ensure that funds are received from respective client only has to be maintained. Necessary details may be collected from banker at which the amount is received.
6. If the pre-paid instrument is received through post or any other method where client does not directly interface for submission of the instrument and the instrument does not contain the information as required above, the following action may be taken:
   - Contact the client immediately and seek information. Not to bank the instrument until the information is given by the client.
   - If the pre-paid instrument is bank transfer, contact banker immediately for the details; not utilize the amount so credited until the details are received/ confirm and not to give credit to the customer until banker gives the details/certification.
7. While giving credit to respective client's ledger, Head office needs to cross check / verify with documents that such instrument is received from respective client's.

Review Policy :
This policy may be reviewed as and when there are any changes introduced by any statutory authority or as and when it is found necessary to change the policy due to business needs.

The policy may be reviewed by the Managing Director/CEO and place the changes in policy before the Board at the meeting first held after such changes are introduced.

Policy communication:
A copy of this policy shall be made available to all the relevant staff who are responsible for receipt of funds from clients and customer service executives.

18

Internal Policy
NISM-Series –VII: Securities Operation and Risk Management Certification Examination

Circulars & References:-

1.SEBI Notification No.LAD-NRO/GN/2010-11/21/29390 published in the Gazette of India on December 10, 2010
2.NSE Circular no. NSE/INSP/16536 December 15, 2010
3.NSE Circular no. NSE/INSP/27495 September 02, 2014
4.BSE Notice no.20101215-19 dated December 15,2010
5.BSE Notice no. 20140902-8 dated September 02,2014

Brief
SEBI issued Notification no. LAD-NRO/GN/2010-11/21/29390 dated December 10, 2010, in which the categories of associated persons associated with a registered stock broker/trading member/clearing member in any recognized stock exchanges, who are involved in, or deal with any of the following:

a. Assets or Funds of investors or clients
b. Redressal of investor grievances
c. Internal control or risk management
d. Activities having a bearing on operational risk

shall be required to have a valid NISM certification of NISM Series VII – Securities Operation & Risk Management (SORM) from National Institute of Securities Market (NISM).

Requirement of the Policy
The Company being a trading member NSE, BSE, MSEI, MCX, NCDEX, ICEX & DP-CDSL , provisions of the aforesaid requirement is applicable to all its employees & sub-brokers involved in the activities as mentioned above.

Definition of "Associated Person"
"Associated Person" means a principal or employee of an intermediary or an agent or distributor or other natural person engaged in the securities business and includes an employee of a foreign institutional investor or a foreign venture capital investor working in India.

Policy
As required in the aforesaid notification of SEBI, all existing persons associated with the Company as on date of publication and engaged in deal with:
(a) Assets of funds of investors or clients
(b) Redressal of investor grievances
(c) Internal control or risk management
(d) Activities having a bearing on operational risk

shall obtain the valid certification of NISM Series VII - Securities Operation and Risk, Management (SORM) within two years from the date of such notification. Simultaneously whenever the company employs any associated person specified as mentioned above, the said associated person shall obtain

valid certification of NISM Series VII – Securities Operation and Risk Management (SORM) within one year from the date of his /her employment/registration as sub-broker.

Exemption

Associated persons handling the basic clerical / elementary functions in the aforesaid specified areas shall be exempted from obtaining the certification of NISM Series VII - Securities Operation and Risk Management (SORM). For this purpose, the company considers following activities as basic elementary lever / clerical level:

Internal Control or Risk Management

- Inwarding or collateral's / Cheques
- Person performing market entries
- Maker entry in the database
- Photocopying, printouts, scanning of documents
- Preparing of MIS
- Sending of letters / reports to clients, Exchanges, SEBI
- Attending Calls, etc.

Redressal of Investor Grievances

- Inwarding of complaints
- Seeking documents from clients
- Person performing maker entries
- Maker entry in the database
- Photocopying, printouts, scanning of documents
- Preparing of MIS
- Sending of letters / reports to clients, Exchanges, SEBI updation, data entry, uploading on SCORES
- Attending calls, etc

Activities having a being on operational risk and dealing with assets of funds of investors of clients

- Person performing maker entries
- Maker entry in the database
- Preparing of MIS
- Generating of reports, Files
- Photocopying, printouts, scanning of documents
- Dispatching documents to clients
- Sending of letters / reports to clients, Exchanges, SEBI
- Attending calls, etc

However, any area (as stated herein above) being performed by the respective persons, obtaining, NISM-SORM Certification shall be optional provided that they are supervised by his / her supervisor who shall have to obtain / continue to have NISM – SORM Certification or such other prescribed certification at all times.

19. POLICIES & PROCEDURE

As per SEBI Circular No: MIRSD/SE/Cir-19/2009 Dated 3rd December, 2009

1. Refusal of orders for penny / illiquid stock

The stock broker may from time to time limit (quantity/value) / refuse orders in one or more securities due to various reasons including market liquidity, value of security(ies), the order being for securities which are not in the permitted list of the stock broker / exchange(s) / SEBI. Provided further that stock broker may require compulsory settlement / advance payment of expected settlement value/ delivery of securities for settlement prior to acceptance / placement of order(s) as well. The client agrees that the losses, if any on account of such refusal or due to delay caused by such limits, shall be borne exclusively by the client alone.

The stock broker may require reconfirmation of orders, which are larger than that specified by the stock broker's risk management, and is also aware that the stock broker has the discretion to reject the execution of such orders based on its risk perception.

2. Setting up client's exposure limits and conditions under which a client may not be allowed to take further position or the broker may close the existing position of a client

The stock broker may from time to time impose and vary limits on the orders that the client can place through the stock broker's trading system (including exposure limits, turnover limits, limits as to the number, value and/or kind of securities in respect of which orders can be placed etc.). The client is aware and agrees that the stock broker may need to vary or reduce the limits or impose new limits urgently on the basis of the stock broker's risk perception and other factors considered relevant by the stock broker including but not limited to limits on account of exchange/ SEBI directions/limits (such as broker level/ market level limits in security specific / volume specific exposures etc.) , and the stock broker may be unable to inform the client of such variation, reduction or imposition in advance. The client agrees that the stock broker shall not be responsible for such variation, reduction or imposition or the client's inability to route any order through the stock broker's trading system on account of any such variation, reduction or imposition of limits. The client further agrees that the stock broker may at any time, at its sole discretion and without prior notice, prohibit or restrict the client's ability to place orders or trade in securities through the stock broker, or it may subject any order placed by the client to a review before its entry into the trading systems and may refuse to execute / allow execution of orders due to but not limited to the reason of lack of margin / securities or the order being outside the limits set by stock broker / exchange/ SEBI and any other reasons which the stock broker may deem appropriate in the circumstances.

a. For Non-Payment or erosion of margins or other amounts, outstanding debts, etc. & adjust the proceeds of such liquidation/ close out if any, against the client's liabilities/obligations.

b. Any order which is executed without the required margin in the client's account or the broker's exposure is more than 90% and above so no fresh trade will be taken.

c. The client hereby authorizes the stock broker to squareup all his outstanding positions at the discretion of the stock broker, which are not marked for delivery, 15 minutes before the closing time of the normal market or if the client's margin is evaporated by 90% in any of the exchange(s), MSB e-Trade reserves the right to square off positions.

d. Under certain market conditions, it may be difficult or impossible to liquidate a position in the market at a reasonable price or at all, when there are no outstanding orders either on the buy side or the sell side, or if trading is halted in a security due to any action on account of unusual trading activity or stock hitting circuit filters or any other reason as prescribed or instructed by SEBI.

The client agrees that the losses, if any on account of such refusal or due to delay caused by such review, shall be borne exclusively by the client alone.

The stock broker is required only to communicate / advise the parameters for the calculation of the margin / security requirements as rate(s) / percentage(s) of the dealings, through anyone or more means or methods such as post / speed post / courier / registered post / registered A.D / facsimile / telegram / cable / e-mail / voice mails / telephone (telephone includes such devices as mobile phones etc.) including SMS on the mobile phone or any other similar device; by messaging on the computer screen of the client's computer; by informing the client through employees / agents of the stock broker; by publishing / displaying it on the website of the stock broker / making it available as a download from the website of the stock broker; by displaying it on the notice board of the branch / office through which the client trades or if the circumstances, so require, by radio broadcast / television broadcast / newspapers advertisements etc; or any other suitable or applicable mode or manner. Once parameters for margin / security requirements are so communicated, the client shall monitor his / her / its position (dealings / trades and valuation of security) on his / her / its own and provide the required / deficit margin / security forthwith as required from time to time whether or not any margin call or such other separate communication to that effect is sent by the stock broker to the client and /or whether or not such communication is received by the client.

The client is not entitled to trade without adequate margin / security and that it shall be his / her / its responsibility to ascertain beforehand the margin / security requirements for his/ her /its orders / trades / deals and to ensure that the required margin / security is made available to the stock broker in such form and manner as may be required by the stock broker. If the client's order is executed despite a shortfall in the available margin, the client, shall, whether or not the stock broker intimates such shortfall in the margin to the client, make up the shortfall suo moto immediately. The client further agrees that he /she / it shall be responsible for all orders (including any orders that may be executed without the required margin in the client's account) & / or any claim /loss/ damage arising out of the non availability /shortage of margin /security required by the stock broker & / or exchange & / or SEBI.

The stock broker is entitled to vary the form (i.e., the replacement of the margin / security in one form with the margin / security in any other form, say, in the form of money instead of shares) & / or quantum & / or percentage of the margin & / or security required to be deposited / made available, from time to time.

The margin / security deposited by the client with the stock broker are not eligible for any interest.

The stock broker is entitled to include / appropriate any / all payout of funds & / or securities towards margin / security without requiring specific authorizations for each payout.

The stock broker is entitled to disable / freeze the account & / or trading facility / any other service, facility, if, in the opinion of the stock broker, the client has committed a crime / fraud or has acted in contradiction of this agreement or / is likely to evade / violate any laws, rules, regulations, directions of a lawful authority whether Indian or foreign or if the stock broker so apprehends.

3. Applicable brokerage rate

The stock broker is entitled to charge brokerage within the limits imposed by exchange which at present is as under:

a. For Cash Market Segment: The maximum brokerage chargeable in relation to trades effected in the securities admitted to dealings on the Capital Market segment of the Exchange shall be 2.5 % of the contract price exclusive of statutory levies. It is hereby further clarified that where the sale / purchase value of a share is Rs.10/- or less, a maximum brokerage of 25 paise per share may be collected.

b. For Option contracts: Brokerage for option contracts would not exceed Rs. 100/- (per lot) single side or such other rates as provided by the exchange(s)/SEBI.

c. For Derivatives contracts: Brokerage for derivatives contracts would not exceed 2.5%/- (per lot) single side or such other rates as provided by the exchange(s)/SEBI.

4. Imposition of penalty / delayed payment charges

Clients will be liable to pay late pay in/delayed payment charges for not making payment of their paying/margin obligation on time as per the exchange requirement/schedule at the rate of 2% per month. The client agree that the Stock broker may impose fine and penalties for the order/ trades/deals/ actions of the clients which is contrary to these agreement/rules/ regulations/ bye laws of the exchange or any other law for the time being in force at such rates and in such form as it may deem fit. Further where the stock broker has to pay any fine or bear any punishment from any authority in connection with/as a consequence of/in relation to any of the orders/trades/deals/actions of the client, the same shall be borne by the client.

The client agrees to pay to the stock broker brokerage, commission, fees, all taxes, duties, levies imposed by any authority including but not limited to the stock exchanges (including any amount due on account of reassessment / backlogs etc.), transaction expenses, incidental expenses such as postage, courier etc. as they apply from time to time to the client's account / transactions / services that the client avails from the stock broker.

5. The right to sell clients' securities or close clients' positions, without giving notice to the client, on account of non-payment of client's dues

The stock broker maintains centralized banking and securities handling processes and related banking and depository accounts at designated place. The client shall ensure timely availability of funds/securities in designated form and manner at designated time and in designated bank and depository account(s) at designated place, for meeting his/her/its pay in obligation of funds and securities. The stock broker shall not be responsible for any claim/loss/damage arising out of non availability/short availability of funds/securities by the client in the designated account(s) of the stock broker for meeting the pay in obligation of either funds or securities. If the client gives orders / trades in the anticipation of the required securities being available subsequently for pay in through anticipated payout from the exchange or through borrowings or any off market delivery(s) or market delivery(s) and if such anticipated availability does not materialize in actual availability of securities / funds for pay in for any reason whatsoever including but not limited to any delays / shortages at the exchange or stock broker level / non release of margin by the stock broker etc., the losses which may occur to the client as a consequence of such shortages in any manner such as on account of auctions / square off / closing outs etc., shall be solely to the account of the client and the client agrees not to hold the stock broker responsible for the same in any form or manner whatsoever.

In case the payment of the margin / security is made by the client through a bank instrument, the stock broker shall be at liberty to give the benefit / credit for the same only on the realization of the funds from the said bank instrument etc. at the absolute discretion of the stock broker. Where the margin /security is made available by way of securities or any other property, the stock broker is empowered to decline its acceptance as margin / security & / or to accept it at such reduced value as the stock broker may deem fit by applying haircuts or by valuing it by marking it to market or by any other method as the stock broker may deem fit in its absolute discretion.

The stock broker has the right but not the obligation, to cancel all pending orders and to sell/close/liquidate all open positions/ securities / shares at the pre-defined square off time or when Mark to Market (M-T-M) percentage reaches or crosses stipulated margin percentage mentioned on the website, whichever is earlier. The stock broker will have sole discretion to decide referred stipulated margin percentage depending upon the market condition. In the event of such square off, the client agrees to bear all the losses based on actual executed prices. In case open position (i.e. short/long) gets converted into delivery due to non square off because of any reason whatsoever, the client agrees to provide securities/funds to fulfill the pay-in obligation failing which the client will have to face auctions

or internal close outs; in addition to this the client will have to pay penalties and charges levied by exchange in actual and losses, if any.
Without prejudice to the foregoing, the client shall also be solely liable for all and any penalties and charges levied by the exchange(s).
The stock broker is entitled to prescribe the date and time by which the margin / security is to be made available and the stock broker may refuse to accept any payments in any form after such deadline for margin / security expires.
Notwithstanding anything to the contrary in the agreement or elsewhere, if the client fails to maintain or provide the required margin/fund / security or to meet the funds/margins/ securities pay in obligations for the orders / trades / deals of the client within the prescribed time and form, the stock broker shall have the right without any further notice or communication to the client to take any one or more of the following steps:
i. To withhold any payout of funds / securities.
ii. To withhold / disable the trading / dealing facility to the client.
iii. To liquidate one or more security(s) of the client by selling the same in such manner and at such rate which the stock broker may deem fit in its absolute discretion. It is agreed and understood by the client that securities here includes securities which are pending delivery / receipt.
iv. To liquidate / square off partially or fully the position of sale & / or purchase in anyone or more securities /
contracts in such manner and at such rate which the stock broker may decide in its absolute discretion.
v. To take any other steps which in the given circumstances, the stock broker may deem fit.
The client agrees that the loss(s) if any, on account of anyone or more steps as enumerated herein above being taken by the stock broker, shall be borne exclusively by the client alone and agrees not to question the reasonableness, requirements, timing, manner, form, pricing etc., which are chosen by the stock broker.

6. Shortages in obligations arising out of internal netting of trades

Stock broker shall not be obliged to deliver any securities or pay any money to the client unless and until the same has been received by the stock broker from the exchange, the clearing corporation/ clearing house or other company or entity liable to make the payment and the client has fulfilled his / her/ its obligations first.
The policy and procedure for settlement of shortages in obligations arising out of internal netting of trades is as under:
a. The securities delivered short are purchased from market on T+2 day which is the Auction Day on Exchange, and the purchase consideration (inclusive of all statutory taxes & levies) is debited to the short
delivering seller client.
b. In case, the shares are not purchased from the market for whatsoever reason, the seller account shall be debited by the closing price of shares on the date of the auction plus 2% over and above the closing price or minimum 50 paise per shares on the date the auction for the settlement which ever is higher.
c. In cases of securities having corporate actions all cases of short delivery of cum transactions which cannot be auctioned on cum basis or where the cum basis auction payout is after the book closure / record date, would be compulsory closed out at higher of 10% above the official closing price on the auction day or the highest traded price from first trading day of the settlement till the auction day.

7. Temporarily suspending or closing a client's account at the client's request

i. The client may request the stock broker to temporarily suspend his account, stock broker may do so subject to client accepting / adhering to conditions imposed by stock broker including but not limited to settlement of account and/ or other obligation.
ii. The stock broker can with hold the payouts of client and suspend his trading account due to his surveillance action or judicial or / and regulatory order/action requiring client suspension.

8. De-registering a client

Notwithstanding anything to the contrary stated in the agreement, the stock broker shall be entitled to terminate the agreement with immediate effect in any of the following circumstances:
i. If the action of the Client are prima facie illegal/ improper or such as to manipulate the price of any securities or disturb the normal/ proper functioning of the market, either alone or in conjunction with others.
ii. If there is any commencement of a legal process against the Client under any law in force;
iii. On the death/lunacy or other disability of the Client;
iv. If a receiver, administrator or liquidator has been appointed or allowed to be appointed of all or any part of the undertaking of the Client;
v. If the Client has voluntarily or compulsorily become the subject of proceedings under any bankruptcy or insolvency law or being a company, goes into liquidation or has a receiver appointed in respect of its assets or refers itself to the Board for Industrial and Financial Reconstruction or under any other law providing protection as a relief undertaking;
vi. If the Client being a partnership firm, has any steps taken by the Client and/ or its partners for dissolution of the partnership;
vii. If the Client have taken or suffered to be taken any action for its reorganization, liquidation or dissolution;
viii. If the Client has made any material misrepresentation of facts, including (without limitation) in relation to the Security;
ix. If there is reasonable apprehension that the Client is unable to pay its debts or the Client has admitted its inability to pay its debts, as they become payable;
x. If the Client suffers any adverse material change in his / her / its financial position or defaults in any other agreement with the Stock broker;
xi. If the Client is in breach of any term, condition or covenant of this Agreement;
xii. If any covenant or warranty of the Client is incorrect or untrue in any material respect;
However notwithstanding any termination of the agreement, all transactions made under / pursuant to this agreement shall be subject to all the terms and conditions of this agreement and parties to this agreement submit to exclusive jurisdiction of courts of law at the place of execution of this agreement by Stock Broker.

Client Acceptance of Policies and Procedures stated here in above:

I/We have fully understood the same and do hereby sign the same and agree not to call into question the validity, enforceability and applicability of any provision/clauses this document any circumstances what so ever. These Policies and Procedures may be amended / changed unilaterally by the broker, provided the change is informed to me / us with through anyone or more means or methods such as post / speed post / courier / registered post / registered AD / facsimile / telegram / cable / e-mail / voice mails / telephone (telephone includes such devices as mobile phones etc.) including SMS on the mobile phone or any other similar device; by messaging on the computer screen of the client's computer; by informing the client through employees / agents of the stock broker; by publishing /

displaying it on the website of the stock broker / making it available as a download from the website of the stock broker; by displaying it on the notice board of the branch / office through which the client trades or if the circumstances, so require, by radio broadcast / television broadcast / newspapers advertisements etc; or any other suitable or applicable mode or manner. I/we agree that the postal department / the courier company /newspaper company and the e-mail/ voice mail service provider and such other service providers shall be my/our agent and the delivery shall be complete when communication is given to the postal department / the courier company / the e-mail/voice mail service provider, etc. by the stock broker and I/we agree never to challenge the same on any grounds including delayed receipt / non receipt or any other reasons whatsoever. These Policies and Procedures shall always be read along with the agreement and shall be compulsorily referred to while deciding any dispute / difference or claim between me/ us and stock broker before any court of law / judicial / adjudicating authority including arbitrator/ mediator etc.

TARIFF SHEET

Segment	Cash Segment				Equity Future & Option Segment				Currency Derivative			
Charges	Square Up Transaction		Delivery Transaction		Future Segment		Option Segment		Currency Future		Currency Option	
	% age	Min. Paise (per share)	% age	Min. Paise (per share	% age	Min. (Per Lot)	% age	Min. (Per Lot)	% age	Min. (Per Lot)	% age	Min. (Per Lot)
Brokerage	%	₹.	%	₹.	%	₹.	%	₹.	%	₹.	%	₹.
Other Charges	%	₹.	%	₹.	%	₹.	%	₹.	%	₹.	%	₹.

Important Note:

- Exchange Turnover Charges, Security Transaction Tax, Stamp Duty, Service Tax, & other Statutory & Govt. Levies are as per applicable by the relevant authority.
- Rs. 25 per may charge as stationary and postage charges in case of dispatching of physical contract note in additional to brokerage, STT or other statutory charges as mentioned above.

******* END *******

20. Policies to Identify or avoid or manage Conflict of Interest

Policy and the objectives

In order to strive for achieving management of conflict of interests, MSB E-TRADE shall endeavor-

- To promote high standards of integrity in the conduct of business
- To ensure fairness of dealing with clients
- To guide for identification, elimination or management of conflict of interest situations
- To provide a mechanism for review and assessment of the policy(ies) on conflict of interests

The conflict of interest policy aims to ensure that the Company's clients are treated fairly and at the highest level of integrity and that their interests are protected at all times. It also aims to identify conflicts of interest between:

- The Company and a Client
- Relevant Person and a Client
- A Company of the Group and a Client
- Two or more Clients of the Company in the course of providing services to these Clients
- A Company service provider and a Client

In addition it aims to prevent conflicts of interest from adversely affecting the interest of its Client.

Conflicts of Interest Policy sets out:

- The Company will identify circumstances which may give rise to conflicts of interest entailing a material risk of damage to our Clients' interests;
- The Company has established appropriate mechanisms and systems to manage those conflicts;
- The Company maintains systems designed to prevent damage to our Clients' interests through identified conflicts.

"Intermediary" and "Associated Person"

Securities and Exchange Board of India (Certification of Associated Persons in the Securities Markets) Regulations,

2007 defines the term "intermediaries" and "associated persons". Accordingly, "intermediary" means an entity registered under SEBI Act and includes any person required to obtain any membership or approval from a stock exchange or a self-regulatory organization; and "associated person" means a principal or employee of an intermediary or an agent or distributor or other natural person engaged in the securities business and includes an employee of a foreign institutional investor or a foreign venture capital investor working in India;

"Conflict of Interest"

Conflicts of Interest can be defined in many ways, including any situation in which an individual or corporation (either private or governmental) is in a position to exploit a professional or official capacity in some way for their personal or corporate benefit. A conflict of interest is a manifestation of the moral hazard problem, particularly when a financial institution provides multiple services and the potentially competing interests of those services may lead to a concealment of information or dissemination of misleading information. A conflict of interest exists when a party to a transaction could potentially make gain from taking actions that are detrimental to the other party in the transaction.

Identification of Conflicts of Interests

The Company shall take adequate steps to identify conflicts of interest. In identifying conflicts of interest, the Company will take into account situations where the Company or an employee or a Relevant Person:

- Is likely to make a financial gain, or avoid a financial loss, at the expense of the Client;
- Has an interest in the outcome of a service provided to the Client or of a transaction carried out on behalf of the Client, which is distinct from the Client's interest in that outcome;
- Has a financial or other incentive to favour the interest of one Client over another;
- Carries out the same business as the Client; or
- Receives from a person other than a Client an inducement in relation to a service provided to a Client, in the form of monies, goods or services, other than the standard commission or fee for that service.

Potential Conflict of Interest

In order to avoid, manage or deal with conflict of interest with the intermediary or the Associated Persons, it is important to identify the possible areas of conflict of interest. MSB E-TRADE lists out the following potential conflict of interest that may affect the company.

- Directorships or other employment;
- interests in business enterprises or professional practices;
- Share ownership;
- Beneficial interests in trusts;
- Personal Account Trading;
- Professional associations or relationships with other organizations;
- Personal associations with other groups or organizations, or family relationships;
- Front running;
- Rebates;
- Kickbacks;
- Commission;
- Where the company carries on the same business as a client;
- Where the company designs, markets or recommends a product or service without properly considering all our other products and services and the interest of all our clients;
- Where the company has a financial or other incentive to favour the interest of another client or group of clients over the interests of a client;

- Where the company has an interest in the outcome of a service provided to, or of a transaction carried out on behalf of, a client which is distinct from that client's interest in that outcome;
- Where the company is likely to make a financial gain or avoid a financial loss at the expense of a client; and
- Where the company receives, or will receive, from the person other than a client an inducement in relation to the service provided to that client in the form of monies, goods or services, other than the standard commission or fee for that service;

Measures to avoid or to deal or manage actual or potential Conflict of Interests

Should a conflict of interest arise, it needs to be managed promptly and fairly. The Company puts in place following arrangements to ensure that:

- There is a clear distinction between the different departments' operations;
- No single person will gather conflicting information, thus counterfeiting or hiding information from investors is minimized;
- The Company's employees are prohibited from investing in a financial instrument for which they have access to non-public or confidential information;
- Transactions by the Company's employees are neither performed nor executed by themselves.
- Employees sign a contract of employment including confidentiality clauses. No associated person may disclose inside information to others, except disclosures made in accordance with the Company's policies and procedures, to other Company personnel or persons outside the Company who have a valid business reason for receiving such information;
- Each department will control the flow of information where, otherwise, the risk of conflict of interest may harm the interest of a Client;
- Relevant information is recorded promptly in a secure environment to enable identification and management of conflicts of interests;
- Adequate records are maintained of the services and activities of the Company where a conflict of interest has been identified;
- In certain jurisdictions appropriate disclosure may be made to the Client in a clear, fair and not misleading manner to enable the Client to make an informed decision;
- There is a periodic review of the adequacy of the Company's systems and controls.
- Employees are required to avoid conflicts of interest with activities they undertake outside MSB E-TRADE.

Information limitations

The Company respects the confidentiality of information it receives regarding its Clients and operates a "Need to Know" approach and complies with all applicable laws in respect of the handling of that information. Access to confidential information is restricted to those who have a proper requirement for the information consistent with the legitimate interest of a Client of the Company. The Company operates internal organizational arrangements to avoid conflicts of interest by controlling, managing or restricting, as deemed appropriate, the flow of confidential information between different areas of business or within a specific division or department. In particular, Chinese Walls are a key tool for conflict of interest prevention, avoiding insider dealing and market manipulation risks. Furthermore, Chinese Walls can involve separation of premises, personnel, reporting lines, files and IT-systems and controlled procedures for the movement of personnel and information between the Company and any

other part of the Company. The Company maintains permanent information barriers between different departments.

Disclosure to clients of possible source or potential areas of conflict of interest (COI):

- MSB E-TRADE or its associated persons should, in writing, disclose to a client any COI in respect of that client including –
- Measures taken to avoid or mitigate the conflict;
- Any ownership interest or financial interest that the provider or representative may be or become eligible for;
- The nature of the relationship or arrangements with a third party that gives rise to a COI in sufficient detail to enable the client to understand the exact nature of the COI.
- MSB E-TRADE or its associated persons should, in writing, inform a client of the policy on Management of Conflict of Interest and how it may be accessed.
- Intimation of an actual or potential COI should be made to a person with responsibility for the issue or area, such as the relevant management team, head of the department or key individual.
- In accordance with an employee's obligation to act in the best interest of MSB E-TRADE, it is not permissible for employees to engage in conduct that would amount to a COI with MSB E-TRADE.
- Staff that fail to disclose a potential or actual COI in accordance with this policy may be liable to disciplinary procedures.
- Where a conflict arises MSB E-TRADE or its Associated Persons will, if it is aware of it, disclose it to a client prior to undertaking trading activity for that client or, if the company does not believe that disclosure is appropriate, to manage the conflict, the company may opt not to proceed with the transaction or matter giving rise to the conflict.
- Where there is no other way of managing a conflict, or where the measures in place do not sufficiently protect Clients' interests, the conflict will be disclosed to allow the Client to make an informed decision on whether to continue using our service in the situation concerned.
- MSB E-TRADE may decline to act for a Client in cases where we believe a conflict of interest cannot be managed in any other way.

Policies and procedures

The Company has developed and implemented policies and procedures throughout its business to prevent or manage potential conflicts of interest. Our employees receive guidance and training in these policies and procedures, and they are subject to monitoring and review processes.

Procedure to comply with the policy

- Every staff member must have a copy of the Policy on management of Conflicts of Interest.
- If a potential COI arises, the transaction must first be discussed with management before entering into the transaction.
- All new employees shall be required to declare their outside interests when they join the firm.
- All staff maintaining personal trading accounts outside of the company are required to instruct their broker to send copy contract notes and periodic statements to the company for reconciliation purposes.

Inducements

The Company does not offer, solicit or accept any inducements, other than the following:

- the fee, commission or benefit which is disclosed to a client, prior to the provision of the relevant service; and
- it is designed to enhance the quality of the relevant service to a client and in line with the Company's duty to act in the best interests of a client.
- Proper fees for the provision of investment services, such as custody costs, settlement and exchange fees, regulatory levies or legal fees, and which cannot give rise to conflicts with the Company's duties to act honestly, fairly and professionally in accordance with the best interests of its clients.

21
CYBER SECURITY AND CYBER RESILIENCE POLICY

INDEX

CYBER SECURITY AND CYBER RESILIENCE POLICY

1. STATUTORY MANDATE This Policy / framework is made based as accordance with the requirements of the SEBI Circular SEBI/HO/MIRSD/CIR/PB/2018/147 ("the circular") dated December 3, 2018.

2. OBJECTIVE OF THE FRAMEWORK The objective of this framework is to provide robust cyber security and cyber resilience to the Stock brokers and depository participants to perform their significant functions in providing services to the holders of securities.

3. APPLICABILITY Provisions of the said circular and framing of cyber security and cyber resilience are required to be complied by all Stock Brokers and Depository Participants registered with SEBI. The policy has been considered, taken on record and approved by the board of directors of the company at their duly convened meeting held on March 7, 2019.

4. SCOPE OF THE FRAMEWORK Cyber-attacks and threats attempt to compromise the Confidentiality, Integrity and Availability (CIA) of the computer systems, networks and databases (Confidentiality refers to limiting access of systems and information to authorized users, Integrity is the assurance that the information is reliable and accurate, and Availability refers to guarantee of reliable access to the systems and information by authorized users). Cyber security framework includes measures, tools and processes that are intended to prevent cyber-attacks and improve cyber resilience. Cyber Resilience is an organization's ability to prepare and respond to a cyber-attack and to continue operation during, and recover from, a cyber-attack. With the view to strengthen and improve Cyber Security and Cyber Resilience framework, the board of directors of the company shall review this policy documents and implementation thereof at least once annually.

5. DESIGNATED OFFICER The company nominates Mr. MUNISH BAJAJ as Designated Officer of the company to assess, identify, and reduce security and Cyber Security risks, respond to incidents, establish appropriate standards and controls, and direct the establishment and implementation of processes and procedures as per the Cyber Security Policy.

6. CONSTITUTION OF TECHNOLOGY COMMITTEE

6.1 The Company constitutes a technology committee ("the committee") with following members:

Sr. No.	Name of the committee Members	Designation of the Members
1	Mr. MUNISH BAJAJ	Designated officer/Chairperson
2	Mr. SATEESH CHANDRA RAI	Member

6.2 Such committee shall on a half yearly basis review the implementation of the Cyber Security and Cyber Resilience policy. Such review shall include but not limited up to, reviewing of current IT and Cyber Security and Cyber Resilience capabilities, setting up of goals for a target level of Cyber Resilience, and establishing plans to improve

and strengthen Cyber Security and Cyber Resilience. The review shall be placed before the Board of directors for taking appropriate action(s), if required.

6.3 The Designated officer and the technology committee shall periodically review instances of cyber-attacks, if any, domestically and globally, and take steps to strengthen Cyber Security and cyber resilience framework.

7. IDENTIFICATION, ASSESSMENT AND MANAGEMENT OF CYBER SECURITY RISK

The company shall ensure the following steps in order to identify, assess, and manage Cyber Security risk associated with processes, information, networks and systems.

7.1 IDENTIFICATION OF CRITICAL IT ASSETS AND RISKS ASSOCIATED WITH SUCH ASSETS The committee and designated officer shall identify the critical assets based on their sensitivity and criticality for business operations, services and data management including various servers, data processing systems, and information technology (IT) related hardware and software etc. The IT team shall maintain up-to-date inventory of its hardware and systems and the personnel to whom these have been issued, software and information assets (internal and external), details of its network resources, connections to its network and data flows.

7.2 PROTECTION OF ASSETS BY DEPLOYING SUITABLE CONTROLS, TOOLS AND MEASURES

In order to protect the cyber safety, the company shall ensure the measures which include, however not limited up to:

- Access controls
- Physical Security
- Network Security Management
- Data security
- Hardening of Hardware and Software
- Application Security in Customer Facing Applications
- Certification of off-the-shelf products
- Patch management •Disposal of data, systems and storage devices
- Vulnerability Assessment and Penetration Testing (VAPT)

The company shall take all such steps to protect assets of the company by deploying suitable controls, tools and measures in conformity with the provisions of SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 3, 2018 and any amendment or substitution thereof. However, the committee and designated officer of the company shall additionally deploy such measures in this respect, as may be warranted from time to time.

7.3 DETECTION OF INCIDENTS, ANOMALIES AND ATTACKS THROUGH APPROPRIATE MONITORING TOOLS/PROCESSES

Necessary steps as may be required to monitor and for early detection of unauthorised or malicious activities, unauthorised changes, unauthorised access and unauthorised

copying or transmission of data / information held in contractual or fiduciary capacity, by internal and external parties shall be maintained, appreciated and taken care on. The security logs of systems, applications and network devices exposed to the internet shall also be, from to time, monitored for anomalies, if any. The company shall ensure high resilience, high availability and timely detection of attacks on systems and networks exposed to the internet, and implement suitable mechanisms to monitor capacity utilization of its critical systems and networks that are exposed to the internet.

7.4 RESPONDING BACK BY TAKING IMMEDIATE STEPS AFTER IDENTIFICATION OF THE INCIDENT, ANOMALY OR ATTACK

The alerts generated from monitoring and detection of systems in order to determine activities that are to be performed to prevent expansion of such incident of cyber-attack or breach, mitigate its effect and eradicate the incident. In case of affection of systems by incidents of cyber-attacks or breaches, the company shall ensure timely restoration of the same in order to provide uninterrupted services. The committee and designated officer shall ensure to have the same Recovery Time Objective (RTO) and Recovery Point Objective (RPO) as per regulatory requirements. With a view to providing quick responses to such cyber-attacks, the committee shall formulate a response plan defining responsibilities and actions to be performed by its employees and support / outsourced staff in the event of cyber-attacks or breach of Cyber Security mechanism. Such plan and any modification therein shall be circulated amongst all the employees and support / outsourced staff from time to time.

7.5 RECOVERY FROM INCIDENT(S) THROUGH INCIDENT MANAGEMENT AND OTHER APPROPRIA TERECOVERY MECHANISMS

The company shall take into account the outcomes of any incident of loss or destruction of data or systems and accordingly shall take precautionary measures to strengthen the security mechanism and improve recovery planning and processes. Periodic checks to test the adequacy and effectiveness of the aforementioned response and recovery plan shall be done.

8. The technology committee in accordance with the provisions of the said circular and formed hereinafter this framework, shall ensure that this framework considers the principles prescribed by National Critical Information Infrastructure Protection Centre (NCIIPC) of National Technical Research Organization (NTRO), Government of India (titled 'Guidelines for Protection of National Critical Information Infrastructure') and subsequent revisions, if any, from time to time.

9. COMMUNICATION OF UNUSUAL ACTIVITIES AND EVENTS IT team of the company under guidance of the committee shall monitor unusual activities and events and shall facilitate communication of the same to designated officer for necessary actions, as may be required.

To prevent the cyber-attacks, the employees, members and participants shall assist the company to mitigate cyber-attacks by adhering the followings:

- To attend the cyber safety and trainings programs as conducted by the company from time to time.

- To endure installation, usage and regular update of antivirus and antispyware software on computer used by them.
- Use a firewall for your Internet connection.
- Download and install software updates for your operating systems and applications as they become available.
- Make backup copies of important business data and information.
- Control physical access to your computers and network components.
- Keep your Wi-Fi network secured and hidden.
- To adhere limited employee access to data and information and limited authority to install software.
- Regularly change passwords.
- Do not use or attach unauthorised devices.
- Do not try to open restricted domains.
- Avoid saving your personal information on computer or any financial data on any unauthentic website.
- To get your computer regularly scanned with anti-virus software.
- Do not release sensitive data of the organization.
- Further the company shall ensure that:
- No person by virtue of rank or position shall have any intrinsic right to access confidential data, applications, system resources or facilities.
- Any access to the systems, applications, networks, databases, etc., shall be for a defined purpose and for a defined period. The company shall grant access to IT systems, applications, databases and networks on a need-to-use basis and based on the principle of least privilege. Such access shall be for the period when the access is required and should be authorized using strong authentication mechanisms.
- An access policy which addresses strong password controls for users' access to systems, applications, networks and databases shall be implemented.
- All critical systems accessible over the internet should have two-factor security (such as VPNs, Firewall controls etc.), as far as possible.
- The company shall ensure that records of user access to critical systems, wherever possible, are uniquely identified and logged for audit and review purposes and such logs would be maintained and stored in a secure location for a time period not less than two (2) years.
- The company shall be required to deploy controls and security measures to supervise staff with elevated system access entitlements (such as admin or privileged users) to company's critical systems. Such controls and measures shall inter-alia include restricting the number of privileged users, if any, periodic review of privileged users' activities, disallow privileged users from accessing systems logs in which their activities are being captured, strong controls over remote access by privileged users, etc.
- Employees and outsourced staff such as employees of vendors or service providers, who may be given authorized access to the critical systems, networks and other computer resources, shall be subject to stringent supervision, monitoring and access restrictions.
- An Internet access policy to monitor and regulate the use of internet and internet based services such as social media sites, cloud-based internet storage sites, etc. within the company's critical IT infrastructure shall be formulated.
- User Management shall address deactivation of access of privileges of users who are leaving the organization or whose access privileges have been withdrawn.
- Physical access to the critical systems shall be restricted to minimum and only to authorized officials. Physical access of outsourced staff / visitors shall be properly supervised by ensuring

at the minimum that outsourced staff / visitors are accompanied at all times by authorized employees.

- Physical access to the critical systems shall be revoked immediately if the same is no longer required.
- The company will ensure that the perimeter of the critical equipments room, if any, shall be physically secured and monitored by employing physical, human and procedural controls such as the use of security guards, CCTVs, card access systems, mantraps, bollards, etc. where appropriate.
- The company shall establish baseline standards to facilitate consistent application of security configurations to operating systems, databases, network devices and enterprise mobile devices within their IT environment. The LAN and wireless networks shall be secured within the premises with proper access controls.
- For algorithmic trading facilities, adequate measures shall be taken to isolate and secure the perimeter and connectivity to the servers running algorithmic trading applications, if any.
- The company shall install network security devices, such as firewalls, proxy servers, intrusion detection and prevention systems (IDS) to protect their IT infrastructure which is exposed to the internet, from security exposures originating from internal and external sources.
- Adequate controls shall be deployed to address virus / malware / ransomware attacks. These controls may include host / network / application based IDS systems, customized kernels for Linux, anti-virus and anti-malware software etc.
- Critical data shall be identified and encrypted in motion and at rest by using strong encryption methods. Illustrative measures in this regard are given in Annexure A and B.
- The company shall implement measures to prevent unauthorized access or copying or transmission of data / information held in contractual or fiduciary capacity. It shall ensure that confidentiality of information is not compromised during the process of exchanging and transferring information with external parties.
- This security policy also covers use of devices such as mobile phones, faxes, photocopiers, scanners, etc., within their critical IT infrastructure, that can be used for capturing and transmission of sensitive data. For instance, defining access policies for personnel, and network connectivity for such devices etc.
- The company shall allow only authorized data storage devices within their IT infrastructure through appropriate validation processes.
- The company shall only deploy hardened hardware / software, including replacing default passwords with strong passwords and disabling or removing services identified as unnecessary for the functioning of the system.
- Open ports on networks and systems which are not in use or that can be potentially used for exploitation of data shall be blocked and measures taken to secure them.
- Application security for Customer facing applications offered over the Internet such as IBTs (Internet Based Trading applications), portals containing sensitive or private information and Back office applications (repository of financial and personal information offered by Brokers to Customers) are paramount as they carry significant attack surfaces by virtue of being available publicly over the Internet for mass use. Required measures for ensuring security in such applications shall be ensured.
- The company shall ensure that off the shelf products, if any, being used for core business functionality (such as Back office applications) should bear Indian Common criteria certification of Evaluation Assurance Level 4. The Common criteria certification in India is being provided by (STQC) Standardisation Testing and Quality Certification (Ministry of Electronics and Information Technology). Custom developed / in-house software and components need not

obtain the certification, but have to undergo intensive regression testing, configuration testing etc. The scope of tests shall include business logic and security controls.

- The company establish and ensure that the patch management procedures include the identification, categorization and prioritization of patches and updates. An implementation timeframe for each category of patches should be established to apply them in a timely manner.
- The company shall perform rigorous testing of security patches and updates, where possible, before deployment into the production environment so as to ensure that the application of patches do not impact other systems.
- Suitable policy for disposal of storage media and systems shall be framed as may be required. The critical data / Information on such devices and systems shall be removed by using methods such as crypto shredding / degauss / Physical destruction as applicable.
- The company shall formulate a data-disposal and data-retention policy to identify the value and lifetime of various parcels of data.
- The company shall regularly conduct vulnerability assessment to detect security vulnerabilities in their IT environments exposed to the internet, as and when required.
- The company with systems publicly available over the internet shall also carry out penetration tests, at-least once a year, in order to conduct an in-depth evaluation of the security posture of the system through simulations of actual attacks on its systems and networks that are exposed to the internet. In addition, the company shall perform vulnerability scanning and conduct penetration testing prior to the commissioning of a new system that is accessible over the internet.
- In case of vulnerabilities discovered in off-the-shelf products (used for core business) or applications provided by exchange empanelled vendors, the company shall report them to the vendors and the exchanges in a timely manner.
- Remedial actions, if required, shall be immediately taken to address gaps that are identified during vulnerability assessment and penetration testing.
- The company shall establish appropriate security monitoring systems and processes to facilitate continuous monitoring of security events / alerts and timely detection of unauthorised or malicious activities, unauthorised changes, unauthorised access and unauthorised copying or transmission of data / information held in contractual or fiduciary capacity, by internal and external parties. The security logs of systems, applications and network devices exposed to the internet shall also be monitored for anomalies, if any.
- Further, to ensure high resilience, high availability and timely detection of attacks on systems and networks exposed to the internet, the company shall implement suitable mechanisms to monitor capacity utilization of its critical systems and networks that are exposed to the internet, for example, controls such as firewalls to monitor bandwidth usage.
- Alerts, if any, generated from monitoring and detection systems shall be suitably investigated in order to determine activities that are to be performed to prevent expansion of such incident of cyber attack or breach, mitigate its effect and eradicate the incident.
- The response and recovery plan of the company shall have plans for the timely restoration of systems affected by incidents of cyber-attacks or breaches, for instance, offering alternate services or systems to Customers. The company shall have the same Recovery Time Objective (RTO) and Recovery Point Objective (RPO) as per regulatory requirements.
- Responsibilities and actions to be performed by company's employees and support / outsourced staff in the event of cyber-attacks or breach of Cyber Security mechanism shall be defined.

- Any incident of loss or destruction of data or systems shall be thoroughly analyzed and lessons learned from such incidents shall be incorporated to strengthen the security mechanism and improve recovery planning and processes.
- Suitable periodic checks to test the adequacy and effectiveness of the aforementioned response and recovery plan shall be done.

11. SUBMISSION OF QUARTERLY REPORTS

Quarterly reports containing information on cyber-attacks and threats experienced, if any, by the company and measures taken to mitigate vulnerabilities, threats and attacks including information on bugs / vulnerabilities / threats that may be useful for other Stock Brokers / Depository Participants shall be submitted to Stock Exchanges / Depositories, as per statutory requirements / guidelines.

12. TRAINING AND EDUCATION

The committee and designated officer shall conduct training and educational sessions for employees to make them aware on building Cyber Security and basic system hygiene awareness, to enhance knowledge of IT / Cyber Security Policy and standards among the employees incorporating up-to-date Cyber Security threat alerts, including to outsourced staff, vendors, if any, and shall take all such steps as may be deemed appropriate by them in this respect.

13. SYSTEMS MANAGED BY VENDORS

Whenever the systems (IBT, Back office and other Customer facing applications, IT infrastructure, etc.) of the company are managed by vendors and the company may not be able to implement some of the aforementioned guidelines directly, the company shall, from time to time, instruct the vendors to adhere to the applicable guidelines in the Cyber Security and Cyber Resilience policy and obtain the necessary self-certifications from them to ensure compliance with the policy guidelines.

14 . SYSTEMS MANAGED BY MIIS Wherever

the applications are offered to customers over the internet by MIIs (Market Infrastructure Institutions), for eg.: NSE's NOW, BSE's BEST etc., the responsibility of ensuring Cyber Resilience on those applications reside with the MIIs and not with the company. In such case, the company is exempted from applying the aforementioned guidelines to such systems offered by MIIs such as NOW, BEST, etc.

15. PERIODIC AUDIT

The company shall arrange to have its systems audited on an annual basis by a CERT-IN empanelled auditor or an independent CISA / CISM qualified auditor to check compliance with the above areas and shall submit the report to Stock Exchanges / Depositories along with the comments of the Board / committee / any committee thereof within three months of the end of the financial year.

Enclosures:

Annexure A: Illustrative Measures for Data Security on Customer Facing Applications

Annexure B: Illustrative Measures for Data Transport Security

Annexure C: Illustrative Measures for Application Authentication Security

Annexure A

Illustrative Measures for Data Security on Customer Facing Applications

1. Analyse the different kinds of sensitive data shown to the Customer on the frontend application to ensure that only what is deemed absolutely necessary is transmitted and displayed.

2. Wherever possible, mask portions of sensitive data. For instance, rather than displaying the full phone number or a bank account number, display only a portion of it, enough for the Customer to identify, but useless to an unscrupulous party who may obtain covertly obtain it from the Customer's screen. For instance, if a bank account number is "123 456 789", consider displaying something akin to "XXX XXX 789" instead of the whole number. This also has the added benefit of not having to transmit the full piece of data over various networks.
3. Analyse data and databases holistically and draw out meaningful and "silos" (physical or virtual) into which different kinds of data can be isolated and cordoned off. For instance, a database with personal financial information need not be a part of the system or network that houses the public facing websites of the Stock Broker. They should ideally be in discrete silos or DMZs.

4. Implement strict data access controls amongst personnel, irrespective of their responsibilities, technical or otherwise. It is infeasible for certain personnel such as System Administrators and developers to not have privileged access to databases. For such cases, take strict measures to limit the number of personnel with direct access, and monitor, log, and audit their activities. Take measures to ensure that the confidentiality of data is not compromised under any of these scenarios.

5. Use industry standard, strong encryption algorithms (eg: RSA, AES etc.) wherever encryption is implemented. It is important to identify data that warrants encryption as encrypting all data is infeasible and may open up additional attack vectors. In addition, it is critical to identify the right personnel to be in charge of, and the right methodologies for storing the encryption keys, as any compromise to either will render the encryption useless.

6. Ensure that all critical and sensitive data is adequately backed up, and that the backup locations are adequately secured. For instance, on servers on isolated networks that have no public access endpoints, or on-premise servers or disk drives that are off-limits to unauthorized personnel. Without up-to-date backups, a meaningful recovery from a disaster or cyber-attack scenario becomes increasingly difficult.

Annexure B
Illustrative Measures for Data Transport Security

1. 1.When an Application transmitting sensitive data communicates over the Internet with the Stock Brokers' systems, it should be over a secure, encrypted channel to prevent Man-In-The-Middle (MITM) attacks, for instance, an IBT or a Back office communicating from a Customer's web browser or Desktop with the Stock Brokers' systems over the internet, or intra or inter organizational communications. Strong transport encryption mechanisms such as TLS (Transport Layer Security, also referred to as SSL) should be used.

2. For Applications carrying sensitive data that are served as web pages over the internet, a valid, properly configured TLS (SSL) certificate on the web server is mandatory, making the transport channel HTTP(S).

3. Avoid the use of insecure protocols such as FTP (File Transfer Protocol) that can be easily compromised with MITM attacks. Instead, adopt secure protocols such as FTP(S), SSH and VPN tunnels, RDP (with TLS) etc.

Annexure C

Illustrative Measures for Application Authentication Security

1. 1.Any Application offered by Stock Brokers to Customers containing sensitive, private, or critical data such as IBTs, SWSTs, Back office etc. referred to as “Application” hereafter) over the Internet should be password protected. A reasonable minimum length (and no arbitrary maximum length cap or character class requirements) should be enforced. While it is difficult to quantify password “complexity”, longer passphrases have more entropy and offer better security in general. Stock Brokers should attempt to educate Customers of these best practices.
2. 2.Passwords, security PINs etc. should never be stored in plain text and should be one-way hashed using strong cryptographic hash functions (e.g.: bcrypt, PBKDF2) before being committed to storage. It is important to use one-way cryptographic hashes to ensure that stored password hashes are never transformed into the original plaintext values under any circumstances.
3. For added security, a multi-factor (e.g.: two-factor) authentication scheme may be used (hardware or software cryptographic tokens, VPNs, biometric devices, PKI etc.). In case of IBTs and SWSTs, a minimum of two-factors in the authentication flow are mandatory.
4. In case of Applications installed on mobile devices (such as smartphones and tablets), a cryptographically secure biometric two-factor authentication mechanism may be used.
5. After a reasonable number of failed login attempts into Applications, the Customer’s account can be set to a “locked” state where further logins are not possible until a password and authentication reset is performed via an out-of-band channel validation, for instance, a cryptographically secure unique link that is sent to the Customer’s registered e-mail, a random OTP (One Time Password) that is sent as an SMS to the Customer’s registered mobile number, or manually by the Broker after verification of the Customer’s identity etc.
6. Avoid forcing Customers to change passwords at frequent intervals which may result in successive, similar, and enumerated passwords. Instead, focus on strong multi-factor authentication for security and educate Customers to choose strong passphrases. Customers may be reminded within reasonable intervals to update their password and multi-factor credentials, and to ensure that their out-of-band authentication reset information (such as e-mail and phone number) are up-to-date.
7. Both successful and failed login attempts against a Customer’s account may be logged for a reasonable period of time. After successive login failures, it is recommended that measures such as CAPTCHAs or rate-limiting be used in Applications to thwart manual and automated brute force and enumeration attacks against logins.

Note: Reference SEBI circular, Exchange’s Circular

22. Policy for outsourcing activities

Purpose & Scope

SEBI Regulations for various intermediaries require that they shall render at all times high standards of service and exercise due diligence and ensure proper care in their operations.

It has been observed that often the intermediaries resort to outsourcing with a view to reduce costs, and at times, for strategic reasons.

Meaning Outsourcing

Meaning Outsourcing may be defined as the use of one or more than one third party – either within or outside the group - by a registered intermediary to perform the activities associated with services which the intermediary offers.

Direction

SEBI vide its circular no. CIR/MIRSD/24/2011 dated December 15, 2011 issued a General Guidelines on Outsourcing of Activities by Intermediaries, SEBI decided to put in place comprehensive guidelines to collectively cover principals for outsourcing for Intermediaries. Core business activities are not to be outsourced by stock brokers.

Principles for outsourcing for intermediaries

1. Assessment of activities to be outsourced
2. Comprehensive outsourcing risk management programme
3. Due diligence of intermediary selected
4. Outlining Outsourcing relationship
5. Confidentiality of the information outsourced
6. Concentration of outsourced services in the hands of a select few third parties Risks involved in outsourcing of activities
    a. Operational risk
    b. Reputational risk
    c. Legal risk
    d. Country risk
    e. Strategic risk
    f. Exit-strategy risk
    g. Counter party risk
    h. Systemic risk

Activities that shall not be Outsourced

MSB e-Trade desirous of outsourcing their activities shall not, however, outsource their core business activities and compliance functions. A few examples of core business activities may be – execution of orders and monitoring of trading activities of clients in case of stock brokers; dematerialisation of securities in case of depository participants; investment related activities in case of Mutual Funds and Portfolio Managers. Regarding Know Your Client (KYC) requirements, the intermediaries shall comply with the provisions of SEBI {KYC (Know Your Client) Registration Agency} Regulations, 2011 and Guidelines issued thereunder from time to time.

We, MSB e-Trade Securities Limited, have at the moment decided not to outsource any functional/ operational activities of the company.

23. SURVEILLANCE POLICY

BACKGROUND

Exchange(s) / Depository(es) vide their circulars Circular No. NSE/SURV/48818 dated July 01, 2021 and Circular Nos *CDSL/OPS/DP/SYSTM/2021/309* dated July 15, 2021 have mandated the need of on-going framework for surveillance obligation of trading members / depository participants and has identified enhancements to make the said earlier framework more effective.

The company has laid down policy guidelines which have been framed in the light of above said circulars, we are adopting and implementing this surveillance policy applicable to both Stock Broking and Depository Participant`s Operations of the company w.e.f. 01.08.2021.

The policy has been approved by its Board of Directors in Board Meeting held at the Registered Office of the company on _____

What is Surveillance?

Surveillance is the process of collecting and analyzing information concerning markets in order to detect unfair transactions that may violate securities related laws, rules and regulations. In order to ensure investor protection and to safeguard the integrity of the markets, it is imperative to have in place an effective market surveillance mechanism. The main objective of the surveillance function is to help maintain a fair and effective market for securities.

Therefore, we have decided to undertake adequate measures for ensuring effectiveness and efficiency of the trading and depository system. The Company with the above motive in mind has framed Surveillance policy focusing on:

i. To establish a surveillance mechanisms and controls in the operations /trading activity
ii. To put in place appropriate controls for the detection and reporting of suspicious trading activities in accordance with applicable laws/laid down procedures.
iii. To comply with applicable laws and regulatory guidelines.

1. Surveillance Policy for Stock Broking Operations:-

i. The Stock Exchange(s) are providing alerts based on predefined criteria to the all the stock brokers through their portals. As per applicable Circulars, the Company is reviewing these alerts and taking appropriate actions after carrying out due diligence viz. either disposing off alerts with appropriate reasons/findings recorded or filing Suspicious Transaction Report (STR) with FIU-India in accordance with provisions of PMLA (Maintenance of records) Rules,2005.

TYPE of TRANSACTIONAL ALERTS DOWNLOADED BY THE EXCHANGE

Sr. No.	Transactional Alerts	Segment
1	Significantly increase in Client Activity	Cash
2	Sudden Trading activity in dormant account	Cash
3	Clients/Group of client(s), deal in common scrips	Cash
4	Client(s)/Group of Client(s) is concentrated in a few illiquid scrips	Cash
5	Client(s)/ Group of Client(s) dealing in scrip in minimum lot size	Cash
6	Client/ Group of Client(s) Concentration in a scrip	Cash
7	Circular Trading	Cash
8	Pump and Dump	Cash
9	Reversal of Trades	Cash & Derivatives
10	Front Running	Cash
11	Concentrated position in the Open Interest/High turnover concentration	Derivatives
12	Order Book Spoofing i.e. large orders away from market	Cash

ii. In addition to above, the company has also implemented the mechanism to generate alerts as per guidance provided in exchange circulars based on following criteria:-

a. Trading activity in a single day by one client or group of clients who have contributed more than 25% in a single scrip or a single derivative contract.
b. A client or a group of clients who are either new client/ clients or who have reactivated their trading account after significant time gap and who have contributed more than 50% of the total trading volume of a single scrip or derivative contract in a single day.
c. Client or a group of clients dealing frequently in small quantities in a scrip.
d. Trading activity of a client found to be disproportionate considering a reported income range details or networth.
e. A client who has submitted modification request for changes in his/her/its demographic details of address, email id, mobile number, bank details etc. at least twice in a month.
f. A client or a group of clients who have been found to have direct or indirect connection with a listed company and who have executed any transactions prior to any dissemination of any price sensitive information by such listed company.
g. A client or group of clients having more than 20% volume of any scrip listed in for 'information list' or 'current watch list'.
h. A client or group of clients which persistently earn or incur high amount of loss through their trading activities or clients who appear to have executed trades with the objective of transfer of profits or losses.
i. A client who is holding more than 5% of paid up capital of a listed company and has pledged 100% of his/her/it's such holding for margin purpose and who has also significant trading volume in the same scrip which he/she/it holds.
j. In case of a client or a group of clients who have been identified as per any of the above criteria and whose orders are placed through a dealing office which is far from such client's address as per his/her/its KYC.
k. A client having demat account with the company and who has holding in a scrip of more than 5% of paid up capital of a listed company which has received the same shares though off-market transfer.
l. A client who has received shares of a listed company through multiple off- market transfer and has pledged such shares.
m. Identification of IP addresses of clients to identify multiple client codes Page 3 of 8 trading from same IP address.
n. Clients who are connected with each other as per key KYC parameters of the clients as updated by respective client.

2, Surveillance Policy for operations as Depository Participant:-

Depositories are providing transactional alerts on biweekly basis based on threshold defined by NSDL / CDSL to the all the DPs report download utility. As per applicable Circular, the company is reviewing these alerts and taking appropriate actions after carrying out due diligence viz. either disposing off alerts with appropriate reasons/findings recorded or filing Suspicious Transaction Report (STR) with FIU-India in accordance with provisions of PMLA (Maintenance of records) Rules,2005.

In addition to the same, company has identified various Surveillance parameters in respect of its operations as Depository Participant to generate alerts as per guidance provided in NSDL / CDSL Circulars based on following criteria:

a. Multiple Demat accounts opened with same PAN/mobile number/ email ID/ bank account details/ address. While reviewing BO account details, the details of existing BO shall also be considered.

b. Email/ letters sent to clients on their registered email ID/address which bounces/ returns undelivered.

c. BO who has submitted modification request for changes in his/her/its demographic details of address, email id, mobile number, bank details, POA holder, Authorised Signatory etc. at least twice in a month.

d. Frequent off-market transfer of securities more than twice in a month without genuine reasons.

e. Off-market transactions not commensurate with the income/networth of the BO.

f. Pledge transactions not commensurate with the income/networth of the BO.

g. High value off-market transfer immediately after modification of either email ID/mobile number/ address without genuine reason.

h. Review of reasons for off-market transfer provided by the BO which appears non-genuine based on either profile of the BO or on account of reason codes, including frequent off-market transfer with reason code gift/donation to unrelated parties and/or with reason code off-market sales.

i. Sudden increase in transaction activity in a newly opened account in a short span of time. An account in which securities balance suddenly reduces to zero and an active account with regular transaction suddenly becomes dormant.

Depository to generate additional surveillance alerts:-

Sr. No.	Indicative themes:
1	Alert for multiple demat accounts opened with same demographic details: Alert for accounts opened with same PAN /mobile number / email id/ bank account no. / address considering the existing demat accounts held with the DP.
2	Alert for communication (emails/letter) sent on registered Email id/address of clients are getting bounced.
3	Frequent changes in details of demat account such as, address, email id, mobile number, Authorized Signatory, POA holder etc.
4	Frequent Off-Market transfers by a client in a specified period
5	Off-market transfers not commensurate with the income/Networth of the client.
6	Pledge transactions not commensurate with the income/Networth of the client.
7	Off-market transfers (High Value) immediately after modification of details in demat account
8	Review of reasons of off-market transfers provided by client for off-market transfers vis-à-vis profile of the client e.g. transfers with reason code Gifts with consideration, frequent transfers with reason code Gifts/Donation to unrelated parties, frequent transfers with reason code off-market sales
9	Alert for newly opened accounts wherein sudden Increase in transactions activities in short span of time and suddenly holding in demat account becomes zero or account becomes dormant after some time.
10	Any other alerts and mechanism in order to prevent and detect any type of market manipulation activity carried out by their clients.

3. PROCESSING AND REVIEW AND DISPOSAL OF ALERTS:-

The surveillance process shall be conducted under overall supervision of its Compliance Officer and he / she shall be the designated official tasked with the review, processing and disposal of alerts.

If the designated official finds after review and due diligence that the alert is required to be closed, the official shall close the same with appropriate remarks.

If the designated official after due diligence and making such inquiry, as such official finds necessary, comes to a conclusion that the given alert warrants an action, the official will forward the same with his/her views to the Designated Director for his/her approval.

In order to review, analyze and dispose off the alerts, the designated official may:-

a. Seek explanation / information from such identified Client(s) / Group of Client(s) for entering into such transactions. Letter/ email to be sent to client asking the client to confirm that client has adhered to trading regulations and details may be sought pertaining to source of funds and securities, economic sense and trading pattern.
b. Seek documentary evidence such as Bank Statement / Demat Transaction Statement, Financial Statements or any other documents to support the trading pattern of the client.

After analyzing the documentary evidences, including the Bank / Demat statement, the observations shall be recorded for such identified transactions or Client(s) / Group of Client(s).

If the designated official finds that action in respect of such alert is warranted, he/she shall take such actions including filing STR with FIU-India, informing to Stock Exchanges and Depository and/or discontinue the relationship with the client.

In case of adverse observations, the report of such instances along with adverse observations and details of actions taken shall be submitted to the Stock Exchanges/ Depository within 7 days from date of identification of such instances.

In case the client does not cooperate or does not revert within reasonable period, Exchange to be informed based on the information available with the member.

All efforts shall be made to dispose off a given alert within 45 days of its receipt / generation.

The records of alerts generated, disposed of as closed and details of action taken wherever applicable shall be maintained with such security measures as would make such records temper proof and the access is available on to designated officials under the supervision of the Compliance Officer.

4. MONITORING AND RECORD MAINTENANCE

The surveillance process shall be conducted under overall supervision of its Compliance Officer and based on facts and circumstances, he / she is required to take adequate precaution.

A quarterly MIS shall be put up by the Compliance Officer to the board and the Designated Director giving number of alerts generated during the quarter, number of alerts closed, number of alerts on which action taken with details of action taken and number of alerts pending at the end of the quarter along with reasons for pendency and action plan for closure. The Board as well as the Designated Director shall be appraised of any exception noticed during the disposal of the alerts

Reasons for pendency shall be discussed and appropriate action would be taken. In case of any exception noticed during the disposition of alerts, the same shall be put up to the Board.

Internal auditor shall review this policy, its implementation, effectiveness and review the alerts generated during the period of audit. Internal auditor shall record the observations with respect to the same in their report.

5. REPORTING OF ALERTS

The Company shall provide duly approved status of the Alerts on a Quarterly basis to the exchange in the format prescribed by the exchange within 15 days from the end of the quarter.

In case zero alert during the quarter, NIL report need to be submit to the exchange as per the prescribed format.

In case, Exchange/Depository provides any transactional alerts, Company shall ask the client to present the documents for clarifying the transaction within the period of 15 days from the date of alert and the same shall be disposed off within the period of 45 days (for Depository within the period of 30 days) and if the same is not disposed off within 45 days of the date of alert, then reason for the same shall be documented.

In case of Proprietary alerts, Company itself shall analyze and review the transactional alerts and disposed off the same within 45 (for Depository within the period of 30 days) days from the date of generation of alerts.

In case of adverse observations are recorded, the Company shall report all such instances to the Exchange within 45 days (for Depository within the period of 30 days) from the date of alert generation.

In case, Depository provides any transactional alerts, Company shall ask the client to present the documents for clarifying the transaction within the period of 15 days from the date of alert and the same shall be disposed off within the period of 45 days (for Depository within the period of 30 days) and if the same is not disposed off within 45 days (for Depository within the period of 30 days) of the date of alert, then reason for the same shall be documented.

6. REVIEW POLICY

This policy will be reviewed by the Designated Director, as and when there are any changes introduced by any statutory authority or atleast once in a year to ensure that same is updated and inline with market trends, updated regulations and practices.

24 POLICY FOR ANTI MONEY LAUNDERING :

Please find separately as per the PMLA policy of the company

25 FINALLY INTERNAL AUDIT, SYSTEM AUDIT & FINANCIAL AUDIT CONDUCT BY THE QUALIFY PERSON LIKE CA, CS, ICWA OR OTHER AUTHORITIES AS PER THE SEBI & EXCHANGE