OPEN FUTURES & COMMODITIES
PRIVATE LIMITED

Company Policies

The information in this document has been classified as "**Confidential**". This classification applies to the most sensitive business information, which is intended strictly for use within **Open Futures& Commodities Pvt**. Ltd. Its unauthorized disclosure could seriously and adversely impact the owner, its stakeholders, its business partners, and/or its customers leading to legal and financial repercussions and adverse public opinion.

INDEX

1. User Management Policy

1. Introduction

1.1. This Policy governs:
1.1.1. The creation, management and deletion of user accounts.
1.1.2. The granting and revocation of authorised privileges associated with a user-account.
1.1.3. The authentication (usually a secret password) by which the user establishes their right to use the account.

2. Scope

2.1. This policy applies to all accounts on computer systems directly connected to networks which are managed by the company. This includes operating system (Windows, Linux etc), and application software etc.
2.2. This document includes statements on:
2.3. Access Control
2.4. Managing Privileges
2.5. Authentication/Password Management

3. Access Control

3.1. The creation, deletion and changes of user accounts and privileges must be carried out by trained and authorised staff.
3.2. The person enacting any change in a user account must be different from the one authorizing/requesting the change.
3.3. An unalterable log will be kept of all account creation/deletion/changes.
3.4. Account details will only be divulged to the user after proof of identity has been established.
3.5. A review period will be established, at an appropriate level for each system, which minimizes information security risks yet allow the company's business activities to be carried out.

4. Managing Privileges

4.1. A user account should have the least privilege which is sufficient for the user to perform their role within the company.
4.2. Changes in the privilege of an account must be authorised by a nominated “owner” of the system to which the account affects.
4.3. Procedures shall be established to ensure that users’ access rights are adjusted appropriately, and in a timely manner, whenever there is a change in business need, a user changes their role, or a user leaves the company.
4.4. Users’ privilege rights will be periodically reviewed.

5. Authentication/Password Management

5.1. All users will have a unique identifier for any company system.
5.2. The user responsible for their account will keep the accounts authentication details secret and will not divulge it to any other person for any reason.
5.3. The account must not be used by the user where there is a possibility that the account details may be revealed.
5.3. Passwords can only be changed by the user or suitably trained and authorised staff.
5.4. If a user suspects their password is no longer secret it must be changed immediately and the system “owner” notified.

6. Document Approval

Approved by: Head of IT Department
Approved Date: 14/10/2016

Review Date: Jan 5th 2013 Reviewer: IT Manager
Review Date: June 5th 2013 Reviewer: IT Manager
Review Date: Aug. 8th 2013 Reviewer: IT Manager
Review Date: Oct. 25th2015 Reviewer: IT Manager
Review Date: Jan. 22nd2016 Reviewer: IT Manager
Review Date: May 19th2016 Reviewer: IT Manager
Review Date: Sep. 21st2016 Reviewer: IT Manager

Appendix 1 – Request for Privileged Access

Name of applicant: _____

Job Title: _____

Permanent
Temporary

Delete as appropriate

Access requested for:

Systems	Login Name	Access Level	Reason

Access required: **From date:** _____
To date: _____

Applicant signature: _____
System owner name: _____
System owner's comments: _____

Approved by: _____
Date :

2. Password Policy

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

2.*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. Access to the resources on the network must be strictly controlled to prevent unauthorized access. Access to all computing and information systems and peripherals shall be restricted unless explicitly authorized.

3. *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 company's any facility, has access to the company's network, or stores any company's non public information. This shall also include Wireless Network also.

4. *Policy*

4.1*General*

4.1.1 All system-level passwords ***(e.g., root, enable, NT admin, application administration accounts, etc.)*** must be changed on at least a **monthly** basis.

4.1.2 All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every one month. The recommended change interval is every fourteen calendar days.

4.1.3 User accounts that have system-level privileges granted through group memberships or programs such as "group" must have a unique password from all other accounts held by that user.

4.1.4 Passwords must not be mentioned into email messages or other forms of electronic communication.

4.1.5 All user-level and system-level passwords must conform to the guidelines described below.
4.2 Trading Application Password

4.2.1 System mandated changing of password when the user logons for the first time.
4.2.2 All admin level, system level shall store in a sealed envelope

4.2.3 Automatic disablement of password on entering erroneous password on three consecutive occasions.

4.2.4*Password shall be alphanumeric and neither only alpha nor only numeric.*

4.2.5*Password shall be change at an interval of fourteen calendar days. 4.2.6 Password shall not be same as last eight passwords.*

4.2.7 Password shall not be same as User Login ID.

4.2.8 Password shall be at least six characters long and not more than twelve characters.

4.2.9 Password shall be automatically disabled on entering erroneous password on three continuous occasions.

5. *Guideline*

5.1 General Password Construction Guidelines
Passwords are used for various purposes. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, and local router logins. 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.

5.1.1 Characteristic of Poor / Weak Password - 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.
- Birthdays and other personal information such as addressesand phone numbers,
- Word or number patterns like aaabbb, qwerty, asdf1234, 123456 etc.
- Any of the above spelled backwards.

5.1.2 Characteristic of Strong Password -

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%A&*()_+ --= \-0[1:";'<>?,. i)
- Are eight alphanumeric characters long.
- Are not words in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered.

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

5.2*Password Protection Standards*
Do not use the same password for accounts as for other l access (e.g., personal ISP account, option trading etc).
Do not share company's passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive and confidential information.
Here is a list of "don'ts":

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name") Don't 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 someone in the Information Security Department.
Do not use the "Remember Password' feature of applications (e.g. Outlook Express, Netscape Messenger).

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 month. The recommended change interval is every fourteen calendar days.
If an account or password is suspected to have been compromised, report the incident to Information Security Personnel and change all passwords.
password is guessed or cracked during one of these scans, the user will be required to change it.

6. *Enforcement*

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

7. *Effective Date*
This policy is effective from 13/09/2012.

8. *Review and Update*

This policy shall be reviewed and updated on an annual basis or on any special event or circumstance.

Password format and general rules are held within the Information Security – A Guide to Staff. Systems logon requires that all passwords be of a minimum of 7 characters.
*Temporary access may be granted on a need to use basis. Such logons may be granted by the ISO (in the Director of xxxxxxxxxxxxx absence) but must be recorded and reported on the normal form. Temporary logons must be identified by a specific login (starting TEMP****) and must be deleted immediately after use.*

3. INTERNAL CONTROL POLICY & RISK MANAGEMENT

Preface:

This document shall deem to be as official guidelines, policies and procedures to be followed by Open Futures while carrying out its business activities as a Member of **MCX** (**Multi Commodity Exchange of India Limited).**

The objective of this document is to effectively manage the various risk involved in the business operations which may include default by clients, fraud and infidelity by employees, technological failures, misuse of trading system for market manipulations apart from protecting the interests of investors and ensuring the effective and timely compliance with various applicable Acts, rules, regulations, bye-laws, circulars and guidelines.

Manner of usage:

This document shall be used as guidelines and reference by the key personnel in charge of the activities namely client identification and introduction, surveillance, record keeping and the personnel in charge of executing and authorizing the day to day transactions as well as by the business associates. Who are involved in the activities as mentioned above. The Compliance Officer (CO) shall provide the copy of this document to all such existing as well as new key Personnel and Business Associates from time to time and explain the contents and their responsibilities in this regard.

1) KRA Policy:

A KRA is a SEBI-registered agency that centrally maintains KYC (Know-Your-Client) records of investors on behalf of Stock broker and other intermediaries. Investors opening new accounts with **Open Futures & Commodities Pvt. Ltd.** will have to complete the KYC formalities only once, which will get uploaded to a KRA. In future if the investor changes the broker, the letter can retrieve the information from a KRA. He need not to undergo KYC process again.

For new client accounts opened after February 1, 2012, the KYC data and requisite documents will be sent to CVL within 10 working days from the date of submission of all documents duly executed by the client. **Open Futures & Commodities Pvt. Ltd.**is registered with CVL, NSE(DotEx)

Details Procedure :

All clients in our Company are allowed to trade only after they have completed the Registration process including the filling of Account Opening Form & KYC Documents (KYC Documents to be done in case of non KRA Registered clients). For Clients who are already registered under KRA a softcopyof the same is download from KRA Authority and we also take fresh KYC and documents with client consent only.

In case of fresh KRA the scanned copy of the same is uploadedto KRA registering Authority forregistration at their end. Further a copy of Rights & Obligations, Risk Disclosure Document,Guidance Note, Policies& Procedures along with a copy of Tariff Sheet is given to clients. Further there are some other documents which are Non-mandatory to be executed byclients at their discretion. Areceipt is taken from the client as a token of his acceptance of all the documents. After verifying the details given by clients, In-person verification is done & the client code is generated and activated in the system.

2) **Risk Management & Internal controls:**

Registration of Clients:-

a. It is a policy of the company to carry client registration in house.
b. KYC procedures as prescribed by MCX/FMC/SEBI/Commodity/Stock Exchange are to be strictly followed while ascertaining the identity and verifying the proof of address of the new clients.
c. No, we do not entertain walk in clients.
d. We take from clientsnetworth / financial standing details which has to be supported by one of the following documents:-

i. Copy of ITR acknowledgement.
ii. Copy of Annual Returns.
iii. Networth certificate from a Chartered Accountant.
iv. Bank Account Statement for last six months.
v. Copy of Demat Account holding statement.
vi. Any other document substantiating ownership of assets.
vii. Identity Proof of Banking Account and Demat account shall be obtained before entering the details of bank and demat account in the client master database.
viii. No we do not outsource client registration modalities.
ix. All client registration documents, once checked, found complete and verified as such and the accounts opened, are securely stored.
x. Yes, we had properly implement the maker-checker concept as a part of our Internal Check system and by virtue of that we duly allocate the work between the two personnel for filling of form and approval of it in order to avoid any misuse of data on unfilled areas.
xi. We have a process of updating of client particulars i.e. address, e-mail id, contact details, etc on request of client in written.
xii. We do UCC though online process after taking on account all due diligence before updating online.
xiii. No, we don't have any separate marketing division.
xiv. No, we never launched any promotional scheme till date.
xv. No, we never offer any freebies to our clients.

3) **Closure of Client accounts/ dormant accounts**

Client Accounts which are lying inactive since last 1 Year months from the account opening date or last transaction date done by client, will be considered as Dormant Accounts and the assets lying therein are returned back. We have categorized them into below mentioned two ways:

One Year dormant Accounts: are those trading accounts in which trading had not placed since last since One Year. In this category , the client code shall be marked disabled in our back office as well as in trading platform, so that no trade can be undertaken/punched in his/her client code. If any such client who is willing to re-initiate trading in its account are required to furnish written request letter of re enablement of its UCC which should be signed by the respective client only & not by POA holder.

Very Old dormant Accounts: are those trading accounts in which trading had not placed since last TWO YEAR. Once the any client code lying inactive since Two years, the client code shall be marked as disabled in our back office as well as in trading platform, so that no trade can be undertaken/punched in his/her client code. If any such client who is willing to re-initiate trading in

its account are required to fulfil KYC formalities along with a written request letter of re-enablement of its UCC which should be signed by the respective client only & not by POA holder.

4) Receiving, validating & entering the orders of clients in the trading platform:-

Normally, the new clients shall be assigned and introduced to a specific terminal operator and the operator shall be briefed about client's requirements for trading, investments and his risk taking abilities. Accordingly the terminal operator shall, under instruction from the concerned senior official.

5) Sending contract notes, daily margin statement, quarterly statement of accounts to clients

a. Asa business practice, at the time of execution of the client agreement, we obtained consent from all our clients regarding the issue of ECN and as per references **circular no. MCX/COMP/087/2014 dated March 19, 2014. Further, w.e.f. December 26, 2014, and Circular no. MCX/COMP/406/2014 dated December 26, 2014**, the Contract Note which are authenticated by means of digital signatures, encrypted and comply with the provisions of the IT Act, 2000 obtained from certifying authority which we send within 24 hours of execution of trades and margin details are send on daily basis to our respective clients, the proof of delivery / dispatch are maintained regularly. Further, in addition to the e-mail communication of the ECNs in the manner stated above, we simultaneously publish the ECN on our designated web site in a secured way and enable relevant access to the clients.

b. Quarterly statement of account along with d-mat holding is send by e-mail. But if client requires statement in physical form we send the statement accordingly.
c. We have maintained the logbook of all the emails which is generated by the system and trail for bounce mails.
d. The Contract Notes, Daily Margin Statement & Quarterly Statement of Accounts of Financial & Securities to clients through email digitally signed within prescribed time frame of exchange on designated email id registered with us.
e. Duplicate copies of contract notes and account statement will be maintained in software itself.

6) Collection and Release of Payments to clients :-

a. The client shall be asked to make the full payment as per the daily debit obligation on T+1 basis. The pay-out of funds shall be made on T+2 bases after confirming the successful pay-in of securities by the client. The exchange/segment wise segregated ledger account shall be maintained with an option to view the exchange position.
b. Under written authorization from the client, the pay-out of funds can be retained for margins and/or future pay-in obligation and for collection and release of funds the account shall be maintained on a running account basis with exchange net balance criteria.
c. No third party transfers are allowed.

7) Collection and maintenance of Margins:-

a. The requirement of collection and maintenance of margins in Cash/Capital Market segment is waived.
b. In case of the clients having relatively large volume and regular trading activities, the pay-out of funds and securities shall be retained towards the upfront and daily margins under the written authorization from the clients.

8) RISK MANAGEMENT

a. The day to day operations are being looked after by the Compliance Officer.
b. The on-line surveillance desk is to be monitored by either of these Senior Officer where real time client wise / scrip wise position, MTM, Margin requirements, available margin and exposure limits will all exchange segment are monitored.
c. Various types of limits on trading terminals are being set up and updated dynamically during the live market.
d. As off line risk management reports are generated which enables to have a quick look at a glance for the status of any individual account or a group of account or for the clients.
e. The various compliance requirements of the exchange / segments shall be ensured by the compliance officers under the supervision of the Senior Officer.

9) Square off of positions / Liquidation of securities without consent of clients

a. Even after regular reminders, if client will fail to make the payment of the margin or pay-in, then we would squared off his/her position and before taking such action in this direction, we telephonically explain all the details to the client about our proposed action in this regard.
b. Principally, company followed the practice of giving reasonable opportunity of being heard and gave a verbal show cause notice to such type of clients, thereafter, if company thinks it is just and reasonable to square off their position, then action will be taken in that direction.

10)Policy of internal shortage

a. The opted policy is in line with exchange recommendations.

11)Transfer of trades

a. Due to efficient fool proof Internal Control System is in place, such type of activities are duly monitored by the authorized persons which restrained the occurrence of any such incident.
b. If sometime punching of order has been done by the dealer, which results in punching the order in the wrong code shall uploaded in UCC as error code.
c. We emphasize our dealers to actively participate in the mock trading sessions organized by the MCX from time to time in order to reduce such instances.

12)Investor Redressal Mechanism

a. The Investor compliant register is maintained as per exchange prescribed format.
b. At the time of opening of account, we informed to our clients about our dedicated investor grievance email & it is printed on KYC too where they can send their grievances.
c. Complaints received, if any, by way of letter, telephonic call, personal representation, e-mail, etc are recorded in the Register of Complaints.
d. Compliance Officer will take care of all those complaints.

13)Allotment /surrender of trading terminals , opening & closing of branches

a. The limit of the clients are fixed subject to Initial Margin deposited or the funds given by the client, Branch or Sub Broker, as the case may be.
b. In case of surrender of terminal, we provide facility to the clients for carrying out trade at other terminal by mapping the same at the earliest.
c. Before any allotment or surrender of any trading terminal, the same will be informed to Exchange via MCX , E-exchange.
d. We monitor the circulars released by the MCX on regular basis in order to ensure that the vendor has still on the panel of MCX with whom we had made tie up for the Internet/CTCL based trading.
e. We do not have any branch & sub-broker.

14) Banking Operations:-

a. All the bank account shall be reconciled on a regular basis by downloading the bank statements in electronic form from the websites of respective banks.
b. One competent employee dedicated for the banking operations shall remain present in or around the clearing bank and ensure the availability of sufficient funds in all the clearing and clients accounts.

15)Continuity planning / alternate plan in case of disasters etc.

a. All the Information Technology infrastructure requirements shall be in charge of the Senior Officer.
b. There shall be sufficient and competent man power to manage the trading system failures during the live market.
c. There shall be the back-up communication link in addition to the regular link for all the exchange segment and it shall be tested periodically.
d. There shall be main line power input from two different routes and there shall be sufficient battery back-up through on-line UPS. Apart from that there shall be a system to quickly switch over to the power back-up through the mobile generator van in case of long power failures.
e. In case of disaster, we can commence the operations from our any of two locations at any time since location have online connectivity, more over we keep back-up zeep, pen drive and cartridges with full data. All our data is loaded on our website which includes client transactions, contracts, ledgers, delivery statement etc. So we are well equipped with our internal system in case of disaster.

16)Detailed policy for client code modification process (including details of personnel authorized to make the modifications, checks in place to ensure that there is no misuse of the facility and escalation of analysis done of client code modifications).

a. The client code of the trades executed by us are modified only in the circumstances that the order entry of the same may be erroneously put into the system by our dealer in wrong client code. After knowing the error done by dealer he has to report immediately the same to Trading In charge who after checking the genuinity of error done by dealer modifies the trades done on the exchange through client code modification facility provided by the exchange. We are not encouraging any type of client code modifications and only genuine errors resulting in trades are modified by us.

b. **Mr. Kuber Singh (RMS-HOD) & Ms. Bhawna Joshi Pandey (Compliance Officer)** is authorised to make such modifications on the exchange platform.

17) Brokerage Charged

Open Futures & Commodities Pvt. Ltd. is entitled to charge brokerage within the limits imposed by exchange which at present is as under:

We ensure that the total brokerage (including our share of brokerage) payable by the client to us does not exceed the maximum brokerage (currently 1% in case of non-delivery transactions and 2% plus expenses in case of transactions relating into delivery) exclusive of statutory levies. (Refer Business Rule 28 and Circular No. MCX/012/2006 dated January 10, 2006). No brokerage is shared with any entity other than registered Authorized Person(s).
We the trading member levy brokerage on all the trades executed on behalf of our clients.
And we do not share brokerage with:-

- Another Member
- An employee of another member or a person for or with whom members are forbidden to do business
- Persons who are not approved users/Authorized Persons

Further, we provide Tariff Sheet (along with Set of Account Opening Document) to our clients while opening their account, which is a document detailing the rate/amount of brokerage and other charges levied on the client for trading on the Commodity Exchange(s).

18) Record Keeping

6.1 Registered intermediaries should ensure compliance with the record keeping requirements contained in the SEBI Act, 1992, Rules and Regulations made there-under, PML Act, 2002 as well as other relevant legislation, Rules, Regulations, Exchange Bye-laws and Circulars.

6.2 Registered Intermediaries should maintain such records as are sufficient to permit reconstruction of individual transactions (including the amounts and types of currencies involved, if any) so as to provide, if necessary, evidence for prosecution of criminal behavior.

6.3 Should there be any suspected drug related or other laundered money or terrorist property, the competent investigating authorities would need to trace through the audit trail for reconstructing a financial profile of the suspect account. To enable this reconstruction, registered intermediaries should retain the following information for the accounts of their customers in order to maintain a satisfactory audit trail:

(a) the beneficial owner of the account;
(b) the volume of the funds flowing through the account; and
(c) for selected transactions:

- the origin of the funds;
- the form in which the funds were offered or withdrawn, e.g. cash, cheques, etc.;
- the identity of the person undertaking the transaction;
- the destination of the funds;
- the form of instruction and authority.

6.4 Registered Intermediaries should ensure that all customer and transaction records and information are available on a timely basis to the competent investigating authorities. Where appropriate, they should consider retaining certain records, e.g. customer identification, account files, and business correspondence, for periods which may exceed that required under the SEBI Act, Rules and Regulations framed there-under PMLA 2002, other relevant legislations, Rules and Regulations or Exchange bye-laws or circulars.

19) PMLA

a. Regular review of procedures and policies on money laundering will be done to ensure its effectiveness.
b. Customers will be sensitized about requirements of provisions emanating from AML and CFT framework.

*We have a detail policy for PMLA.

4. Access Control Policy

1. ***OVERVIEW***

Access control is the selective restriction of access to a place or other resource. The act of accessing may mean consuming, entering, or using. Permission to access a resource is called authorization.

2. ***BACKGROUND***

Resource managers to establish user access controls to protect information resources. Such controls will be based on the principle of least privilege, defined as granting the most restrictive authority so that users are not allowed to undertake actions beyond what their duties require. User access issues also involve In formation Categorization issues addressed.

3.***GUIDING PRINCIPLES***

- Users will have access to the resources needed to accomplish their duties.
- User access applies the principles of least privilege and resource categorization as necessary tools to achieve the desired purpose
- User access controls will balance security and mission needs.

4. ***POLICY***

All managers of information resources will ensure access to information is properly authorized and granted with correct access levels and privileges applied.

4.1 ***Operational Definitions***

4.1.1*Authentication*: Verification that the user's claimed identity is valid and is usually implemented through a user password at logon.

4.1.2 *Discretionary User Access*: The ability to manipulate data using customer general-purpose programs. The only in formation logged for discretionary control mechanisms is the type of data accessed and at what level of authority.

4.1.3 *Identification*: The act of a user professing an identity to a system, usually in the form of a logon to the system.

4.1.4 *Non-discretionary User Access*: The access obtained in the process of specific business transactions that affect information in a pre-defined way. deployment specialists need to access participant information to make travel arrangements but may not need the ability to change any existing information.

4.1.5 *Password*: An arrangement of characters entered by a system user to substantial their identity, authority, and access rights to an information system they wish to use.

4.1.6 *Privilege*: The level of user authority or permission to access information resources. Privileges can be established at the folder, file, or application levels, or for other conditions as applicable.

4.1.7*Special User Access Privileges*: Privileges that allow users to perform specialized tasks that require broad capabilities. For example, changing control functions such as: access control, logging, and violation detection, require special access privileges.

4.1.8*User Account*: An issued name with authority, granted to an individual to access a system or software application. System administrators, with proper management approval, typically grant user accounts. To access an account, a user needs to be authenticated, usually by providing a password.

4.1.9*User Access Controls*: The rules and deployment of mechanisms, which control access to information resources, and physical access to premises.

4.2*User Accounts*

The creation of a user account must be initiated through a request from personnel authorized to approve access to the specified resources, typically a manager or supervisor.

4.3 *Account Management*

Each participant organization manages user accounts for systems within there are a of responsibility. Records of processed and denied requests for creation of user accounts must be kept for auditing purposes. Records will be retained for one year.

4.4 *User Accounts Characteristics*

All user accounts must be unique, and traceable to the assigned user. All participant organizations will take appropriate measures to protect the privacy of user information associated with user accounts. The use of group accounts and group passwords is not allowed.

4.5 *Password Reset*

Each participant organization will establish a procedure for verifying a user's
Identity prior to resetting their password.

4.6 *User Account Privileges*

Users will be granted the minimum access required to perform their specific tasks. Granting access levels to resources shall be based on the principle of least privilege, job responsibilities, and separation of duties. The level of minimum access requires the recommendation of the user's manager, and the evaluation of the information system owner. The information system owner will have final determination as to the level of a user's access for their system.

4.7 *Inactive Accounts*

Accounts will be disabled after 30 days of inactivity. Users planning to deploy to field operating locations or to be away from the office for other approved periods of extended absence should coordinate their absence with the account manager to ensure proper disposition of the account.

4.8 *Temporary User Accounts*

All requests for temporary user accounts shall provide an expiration date to be applied at the time the account is created.

4.9 *Password Characteristics*

All passwords must be constructed using the following characteristics: alphanumeric characters, with a mixture of letters, numbers and special characters. Each participant organization will implement appropriate procedures and technology to enforce this requirement.

4.10 *Automatic Logon*

The use of automatic log on software to circumvent password entry shall not be allowed, except with specific approval from the Information Security Manager, for special tasks such as automated backups.

4.11 *User Account and Password Safekeeping*

Each individual assigned a user account and password is responsible for the actions taken under said account, and must not divulge that account information to any other person for any reason

4.12 *Management Access to User Accounts*

Management access to user accounts will be limited to business purposes only, such as during an emergency or contingency situation, cases of extended user absence, or user abuse of information resources. Each participant organization will establish procedures for providing their management with access to accounts assigned to a user within their organization.

4.13 *Transfers*

Personnel transferring from one area of responsibility to another, shall have their access accounts modified to reflect their new job responsibilities.

4.14 *User Access Cancellation*

Each participant organization will implement procedures to immediately cancel account access and physical access for users whose relationship with the concluded, either on friendly or unfriendly terms.

4.15*User Session Time-out*

User sessions will time-out after15 minutes of inactivity unless otherwise specified as part of the system or application security plan. This includes user connections to the Internet, or to specific applications.

4.16*Remote Access Security*
Access points for remote computing devices shall be configured using necessary identification and authentication technologies to meet security levels of physically connected computers.

4.17*New Information Systems*
All new information systems acquired or by organizations to support program requirements will incorporate access controls to properly protect the information resources.

4.18*Sensitive Information Access*
Individuals for positions with access to sensitive information will be screened for best suitability to the position. These individuals will be subject to the provisions of policies and procedures to protect and safeguard such information from unauthorized disclosure.

4.19*Temporary Access to Sensitive Resources*
Temporary access to resources categorized as sensitive will be set with expiration dates where possible. The system owner will monitor temporary access to ensure activities comply with the intended purpose.

5.*APPLICABILITYAND COMPLIANCE*
This policy applies to all information resources, systems, and technology and to all users of these resources, systems and technology with in the operating environment or connected to the information infrastructure.

6.*RESPONSIBILITIES*
6.1*Information Security Manager (ISM)*

The ISM coordinates the activities of participant organizations in the implementation of this policy.

6.2*Participant Organizations*
Each participant organization will establish procedures to implement these requirements.

7.*PROGRAM IMPLEMENTATION*
Each participant organization will establish processes and procedures to implement this policy, and coordinate their activities with the Information Security Manager.

7.1*User Access Administration*
The information system owner has primary management responsibility for administering user access to information resources. The information system owners in each participant organization will coordinate their activities with the Information Security Manager.

5. Backup Policy and Restoration

1. ***OVERVIEW***
The Company is in the business of Securities Market Braking and uses Front end Trading System and Back Office system (hereafter referred as "network") to expand its network and facilitate clients.
Back up is an important aspect of computer data security. This policy defines the backup policy for computers owned and operated by company which are expected to have their data backed up. These systems are typically servers but are not necessarily limited to servers. Servers expected to be backed up include the database server, the application server, the mail server, and the web server.

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

3. *Scope*
This policy applies to all equipment and data owned and operated by Company.

4. *Definitions*

4.1 *Backup* - The saving of files onto magnetic tape or other offline mass storage media for the purpose of preventing loss of data in the event of equipment failure or destruction.

4.2 *Archive* - The saving of old or unused files onto magnetic tape or other offline mass storage media for the purpose of releasing on-line storage room.
4.3 *Restore* - The process of bringing off line storage data back from the offline media and putting it on an online storage system such as a file server.

5. *Timing*
The data of the Critical Servers shall be backed up on a daily basis on all working days.

6. *Policy*

6.1 *General Back up Policy:*

6.1.1 Daily Integrated back up of all data in database server, web server, application server 86 mail server, operating system and utility files including all patches, fixes and updates shall be taken on a daily basis.
6.1.2*Media:* The media on which the backup shall be taken may comprise of External Hard Disks, Tapes, or any other media being used by the company.

6.1.3 The back-up media should be labeled with information related to data stored, server name and the type of data.

6.1.4 Back up data shall be stored on site in a fire proof cabinet and a copy of the same shall be at maintained at an offsite location.

6.2 *Guideline for Back up:*

The following registers should be maintained and signatures of the responsible persons should be taken with date and time stamp:

a) Inward/Outward Register for Backup Media
b)

Date	Handover Time	Particulars of Media And Data therein	Name of the person delivering the media	Sender's Signature	Name of the receiver	Receiver's Signature

c) *Back-up Register*

Date and Time	Name of the Person Responsible	Nature of Data backup	Signature

7. Back-up Procedure Open Futures & Commodities Pvt. Ltd. Follows:-

The IT administrator shall ensure that the following servers, applications and databases are backed-up compulsorily

PLEASE *ENTER THE DATA OF OUR DRIVES AND SERVER*

Back up procedures

Name of the Server	I/P address	File Location	Frequency of Backup
Trading Server			
Swin	10.43.164.49	MCX_BACKUP/164.49	Weekly
Red	10.43.164.31	MCX_BACKUP/164.31	Weekly
White	10.43.164.94	query/<Trading Date>	Daily
Rea	10.43.164.22	query/<Trading Date>	Daily
Wye	10.43.164.85	MCX_BACKUP/164.85	Weekly
Wapti	10.43.164.103	MCX_BACKUP/164.103	Weekly
Murray	10.43.164.4	MCX_BACKUP/164.4	Weekly
Slizza	10.43.164.13	MCX_BACKUP/164.13	Weekly
Newton	10.43.164.112	MCX_BACKUP/164.112	Weekly
Tejaswi5	10.43.166.13	MCX_BACKUP/166.13	Weekly
Satluj	10.43.166.130	MCX_BACKUP/166.130	Weekly
Vaigi	10.43.166.146	MCX_BACKUP/166.146	Weekly
Dhruv	10.43.166.49	MCX_BACKUP/166.49	Weekly

Tapti2	10.43.166.22	MCX_BACKUP/166.22	Weekly
Alaknanda	10.43.166.122	MCX_BACKUP/166.122	Weekly
Backoffice Servers			
RMS-Node	10.43.160.27	D:\Backup\Database name – DDMMYYYY.dat	**Daily**

The back-up of the *trading files is transferred to a separate back-up server on every Saturday* i e. on a *weekly basis The*back-up on *the database server and trading server are copied to* a *separate HDD* on a *monthly basis.*
The updates and releases are received through e-mail and are accessed by the authorized person. The older version of the application is backed-up.

8 ***Responsibilities***

IT department takes care of all computers' data and strictly follow the aforesaid backup procedure. The IT department manager delegates a member of the IT department to perform regular backups. He keeps the data backup safely and even maintains a separate physical register having written all recorded of when backup being taken and the name of accountable person for that.The delegated person alsodevelops a procedure for testing backups and test the ability to restore data from backups on a monthly basis.

9 ***Testing***

The integrity of the data is tested at the time of backing-up by enabling the integrity check function. The data stored on the backup server may be tested at the time of mock trading.

10 ***Archives***

Archives are made at the end of every quarter in March, June, September and December. User account data associated with the file and mail servers are archived one month after they have left the organization.

11 Restoration

in order to restore the files user must submit a written request to the IT department which shall be authorised by head of the relevant department. Request should also state the file creation date, the name of
the file, the last time it was changed, and the date and time it was deleted or destroyed.

12 Review and update

This policy shall be reviewed and updated on a half yearly basis or on any special event or circumstance.

6. Audit Trail Policy

1. *Overview*
The Audit trails maintain a record of all actions on resources by individuals and computing programs and processes.

2.*Purpose*
The purpose of the policy is round the clock tracking of resource usage, detailed monitoring of employee activity, real time event logging and so on.

3.*Policy*

3.1 The functions that shall be recorded are; log-in attempts, password changes, file creations, changes and/or deletions and so on.
3.2 The audit trail event record shall specify type of event, occurrence of event, user ID associated with the event and program or command used to initiate the event.

4. *Component of Audit Trail Policy*
The following are the components of the audit trail policy:
4.1 A regular back-up of the audit log files shall be taken to fix the accountability for usage of resources on individuals, enable reconstruction of events, intrusion detection and enable analysis of problems and failed events.
4.2 Audit trails shall be reviewed on a regular basis and corrective action shall be taken based on audit trail information.
4.3 A proper register shall be maintained for the back-up of the audit trail and the person responsible shall put his initials on it.

5.*Review*
Audit trails shall be reviewed weekly by the Security Officer or other authorized individuals or who do not administer access to the database. Management must review the audit trail monthly.

6. *Reporting*
Anomalies shall be immediately reported to appropriate supervisory and/or management for follow-up action. In case of anomalies of serious nature a committee shall be set up for further investigation. The relevant department head shall be a part of the Investigating Team. In case of the scrutiny of activities of the department head any other person designated by the Managing director shall be a part of the investigating team.

7.*Compliance*
Unauthorized personnel are not allowed to verify or obtain sensitive data. The gross negligence or willful disclosure of information shall result in prosecution resulting in **fines** and/or dismissal.

8. *Storage*
All audit files shall be stored in a locked room and kept for ten years.

9.*Review and Update*

This policy shall be reviewed and updated on an annual basis or on, any special event or circumstance.

7. Information Security Policy

1. *POLICY STATEMENT*

"It shall be the responsibility of the LT. Department to provide adequate protection and confidentiality of all corporate data and proprietary software systems, whether held centrally, on local storage media, or remotely, to ensure the continued availability of data and programs to all authorised members of staff, and to ensure the integrity of all data and configuration controls."

Summary of Main Security Policies.

1.1. Confidentiality of all data is to be maintained through discretionary and mandatory access controls.

1.2. Internet and other external service access is restricted to authorised personnel only.

1.3. Access to data on all laptop computers is to be secured through encryption or other means, to provide confidentiality of data in the event of loss or theft of equipment.

1.4. Only authorised and licensed software may be installed, and installation may only be performed by I.T. Department staff.

1.5. The use of unauthorized software is prohibited. In the event of unauthorized software being discovered it will be removed from the workstation immediately.

1.6. Data may only be transferred for the purposes determined in the Company's data-protection policy.

1.7. All diskette drives and removable media from external sources must be virus checked before they are used within the Company.

1.8. Passwords must be as per Password Policy.

1.9. Workstation configurations may only be changed by I.T. Department staff.

1.10. The physical security of computer equipment will conform to recognized loss prevention guidelines.

1.11. To prevent the loss of availability of IT. resources measures must be taken to backup data, applications and the configurations of all workstations.

1.12 A business continuity plan will be developed and tested on a regular basis.

2. ***VIRUS PROTECTION***

2.1. The I.T. Department will have available up to date virus scanning software for the scanning and removal of suspected viruses.

2.2. Corporate file-servers will be protected with virus scanning software. 2.3. Workstations will be protected by virus canning software.

2.4. All workstation and server anti-virus software will be regularly updated with the latest anti-virus patches by the I.T. Department.

2.5. No disk that is brought in from outside the Company is to be used until it has been scanned.

2.6. All systems will be built from original, clean master copies whose write protection has always been in place. Only original master copies will be used until virus scanning has taken place.

2.7. All removable media containing executable software (software with .EXE and .COM extensions) will be write protected wherever possible.

2.8. All demonstrations by vendors will be run on their machines and not the Company's.

2.9. Shareware is not to be used, as shareware is one of the most common infection sources. If it is absolutely necessary to use shareware it must be thoroughly scanned before use.

2.10. New commercial software will be scanned before it is installed as it occasionally contains viruses.

2.11. All removable media brought into the Company by field engineers or support personnel will be scanned by the IT Department before they are used on site.

2.12. To enable data to be recovered in the event of a virus outbreak regular backups will be taken by the IT. Department.

2.13. Management strongly endorse the Company's anti-virus policies and will make the necessary resources available to implement them.

2.14. Users will be kept informed of current procedures and policies.

2.15. Users will be notified of virus incidents.

2.16. Employees will be accountable for any breaches of the Company's anti-virus policies.

a. Anti-virus policies and procedures will be reviewed regularly.

2.18. In the event of a possible virus infection the user must inform the I.T. Department immediately. The I.T. Department will then scan the infected machine and any removable media or other workstations to which the virus may have spread and eradicate it.

2. PHYSICAL SECURITY OF COMPUTER EQUIPMENT

Physical Security of computer equipment will comply with the guidelines as detailed below.

3.1. DEFINITIONS

3.1.1.*AREA*
Two or more adjacent linked rooms which, for security purposes, cannot be adequately segregated in physical terms.

3.1.2.*COMPUTER SERVER ROOM*
Mainframe, minicomputer, fileserver plus all inter-connected wiring, fixed disks, telecommunication equipment, ancillary, peripheral and terminal equipment linked into the mainframe, contained within a purpose built computer Server Room.

3.1.3.*COMPUTER EQUIPMENT*
All computer equipment not contained within the COMPUTER SERVER ROOM which will include PC's, monitors, printers, disk drives, modems and associated and peripheral equipment.

3.1.4.*HIGH RISK SITUATION(S)*
This refers to any room or area which is accessible

- At ground floor level
- At first floor level, but accessible from adjoining roof
- At any level via external fire escapes or other features providing access
- Rooms in remote, concealed or hidden areas

3.1.5.*LOCKDOWN DEVICE(S)*
A combination of two metal plates, one for fixing to furniture, or the building structure, and the other for restraining the equipment which is immobilised when the two plates are locked together. The plate for restraining the equipment should incorporate an enclosure or other mechanism which will hinder unauthorised removal of the outer PC casing and render access to internal components difficult.

3.1.6.*APPROVED*
Approved security system.

3.1.7.*PERSONAL COMPUTERS (PC's)*
Individual computer units with their own internal processing and storage capabilities.

3.2.1*Security Marking*
All computer hardware should be prominently security marked by branding or etching with the name of the establishment and area postcode. Advisory signs informing that *all* property has been security marked should be prominently displayed externally.

The following are considered inferior methods of security marking; text comprised solely of initials or abbreviations, marking by paint or ultra violet ink (indelible or otherwise), or adhesive labels that do not include an etching facility.

3.2.2*Locking of PC cases*
PC's fitted with locking cases will be kept locked at all times.

3.2.3. *Sitting of Computer*
Wherever possible, **COMPUTER EQUIPMENT** should be kept at least 1.5 metres away from external windows in **HIGH RISK SITUATIONS.**

3.2.4. *Opening Windows*
All opening windows on external elevations in **HIGH RISK SITUATIONS** should be fitted with key operated locks.

3.2.5 *Blinds*
All external windows to rooms containing **COMPUTER EQUIPMENT** at ground floor level or otherwise visible to the public should be fitted with window blinds or obscure filming.

3.2.6. *Lockdown Devices*

For any item of **COMPUTER EQUIPMENT** with a purchase price in excess of 1,500 which is not directly covered by an intruder alarm, the processing unit should have a **LOCKDOWN DEVICE** fitted to the workstation.
LOCKDOWN DEVICES should conform to loss prevention standards. Mobile workstations are unlikely to be suitable for these devices.
When it is impossible or undesirable to anchor hardware, such equipment can be moved to a security store or cabinet outside normal hours of occupation.

3.2.7. *Intruder Alarm*
An intruder alarm incorporating the following features should be installed. installation, maintenance and monitoring by an **APPROVED** company.

3.2.8. *Check Detectors*
Building managers should ensure, as part of their normal duties at locking up time, that internal space detectors have not been individually obscured nor had their field of vision restricted.

3.3. COMPUTER SERVER ROOM

3.3.1. The computer Server Room should be housed in a purpose builtroom.

3.3.2. There shall not be Wooden Walls **or** Wooden Floorings.

3.3.3. Secure doors giving access to the room or **AREA,** from within the building, should be solid.

3.3.4. The computer Server Room should contain an adequate air conditioning system to provide a stable operating environment to reduce the risk of system crashes due to component failure.

3.3.5. No water, rain water or drainage pipes should run within or above the computer Server Room to reduce the risk of flooding.

3.3.7. Power points should be raised from the floor to allow the smooth shutdown of computer systems in case of flooding.

3.3.8. Where possible generator power should provided to the computer Server Room to help protect the computer systems in the case of a mains power failure.

3.3.9. Access to the computer Server Room is restricted to IT Department staff.

3.3.10. A1l contractors working within the computer Server Room are to be supervised at all times and the It Department is to be notified of their presence and provided with details of all work to be carried out at least 48 hours in advance of its commencement.

4 ACCESS CONTROL

4.1. Users will only be given sufficient rights to all systems to enable them to perform their job function. User rights will be kept to a minimum at all times.

4,2. Users requiring access to systems must make a written application on the forms provided by the LT Department.

4.3. Where possible no one person will have full rights to any system. The I.T. Department will control network/server passwords and system passwords will be assigned by the system administrator in the end-user department. The system administrator will be responsible for the maintaining the data integrity of the end-user department's data and for determining end-user access rights.

4.4. Access to the network/servers and systems will be by **individual** username and password, or by smartcard and PIN number/barometric.

4.5. Usernames and passwords must not be shared by users.

4.6. Usernames and passwords should not be written down.

4.7. Usernames will consist of initials and surname.

4.8. All users will have password as per Password Policy.
4.9. Access to the network/servers will be restricted to normal working hours. Users requiring access outside normal working hours must request such access in writing on the forms provided by the I.T. Department.

4.10. File systems will have the maximum security implemented that is possible. Where possible users will only be given Read and File scan rights to directories, files will be flagged as read only to prevent accidental deletion.

5. ***LAN Security***

Hubs & Switches

5.1. LAN equipment, hubs, bridges, repeaters, routers, switches will be kept in secure hub rooms. Hub rooms will be kept locked at all times. Access to hub rooms will be restricted to LT. Department staff only. Other staff, and contractors requiring access to hub rooms will notify the I.T. Department in advance so that the necessary supervision can be arranged.

Workstations

5.2. Users must logout of their workstations when they leave their workstation for any length of time. Alternatively Windows workstations may be locked.
5.3. All unused workstations must be switched off outside working **hours.**

Wiring

5.4. All network wiring will be fully documented.
5.5. All unused network points will be de-activated when not in use.
5.6. All network cables will be periodically scanned and readings recorded for future reference.
5.7. Users must not place or store any item on top of network cabling.
5.8. Redundant cabling schemes will be used where possible, Monitoring Software
5.9. The use of LAN analyser and packet sniffing software is restricted to the I.T. Department.
5.10. LAN analysers and packet sniffers will be securely locked up when not in use.
5.11 Intrusion detection systems will implemented to detect unauthorised access to the network

Servers

5.12. All servers will be kept securely under lock and key.
5.13. Access to the system console and server disk/tape drives will be restricted to authorised I.T. Department staff only.

Electrical Security

5.14. All servers will be fitted with **UPS's** that also condition the power supply.
5.15. All hubs, bridges, repeaters, routers, switches and other critical network equipment will also be fitted with UPS's.
5.16. In the event of a mains power failure, the UPS's will have sufficient power to keep the network and servers running until the

generator takes over.
5.17. Software will be installed on all servers to implement an orderly shutdown in the event of a total power failure.
5.18. All UPS's will be tested periodically.

Inventory Management

5.19. The I.T. Department will keep a full inventory of all computer equipment and software in use throughout the Company.
5.20. Computer hardware and software audits will be carried out periodically via the use of a desktop inventory package. These audits will be used to track unauthorised copies of software and unauthorised changes to hardware and software configurations.

6. *Server Specific Security*
This section applies to Windows, UNIX, Linux and Novell servers.

6.1. The operating system will be kept up to date and patched on a regular basis.
6.2. Servers will be checked daily for viruses.
6.3. Servers will be locked in a secure room.
6.4. Where appropriate the server console feature will be activated.
6.5. Remote management passwords will be different to the Admin/Administrator root password.
6.6. Users possessing Admin/Administrator root rights will be limited to trained members of the I.T. Department staff only.
6.7. Use of the Admin/Administrator root accounts will be kept to a minimum.
6.8. Assigning security equivalences that give one user the same access rights as another user will be avoided where possible.
6.9. Users access to data and applications will be limited by the access control features.
6.10. Intruder detection and lockout will be enabled.
6.11. The system auditing facilities will be enabled.
6.12. Users must logout or lock their workstations when they leave their workstation for any length of time.
6.13. All unused workstations must be switched off outside working hours.
6.14. All accounts will be assigned a password as per Password Policy.
6.15. The number of concurrent connections will be limited to 1.
6.16. Network login time restrictions will be enforced preventing users from logging in to the network outside normal working hours.
6.17. In certain areas users will be restricted to logging in to specified workstations only.

Area Network Security

7.1. Wireless 'LAN's will make use of the most secure encryption and authentication facilities available. Users will not install their own wireless equipment under any circumstances.
7.3. Dial-in moderns will not be used if at all possible. If a modem must be used dial-back modems should be used. A secure VPN tunnel is the preferred option.
7.4. Modems will not be used by users without first notifying the I.T. Department and obtaining their approval.
7.5. Where dial-in modems are used, the modem will be unplugged from the telephone network and the access software disabled when not in use.

7.6 Modems will only be used where necessary, in normal circumstances all communications should pass through the Company's router and firewall.
7.7. Where leased lines are used, the associated channel service units will be locked up to prevent access to their monitoring ports.
7.8. All bridges, routers and gateways will be kept locked up in secure areas.
7.9. Unnecessary protocols will be removed from routers.
7.10 The preferred method of connection to outside Companies is by a secure VPN connection, using IPSEC or SSL.
7.11 All connections made to the Company's network by outside Companies will be logged.

8. ***TCP/IP Internet Security***

8.1. Permanent connections to the Internet will be via the means of a firewall to regulate network traffic.
8.2. Permanent connections to other external networks, for offsite processing etc., will be via the means of Afire wall to regulate network traffic.
8.3. Where firewalls are used, a dual homed firewa_11 (a device with more than one TCP/IP address) will be the preferred solution.
8.4. Network equipment will be configured to close inactive sessions.
8.5. Where modem pools or remote access servers are used, these will be situated on the DMZ or non-secure network side of the firewall. Workstation access to the Internet will be via the Company's proxy server and web site content scanner
8.7 All incoming e-mail will be scanned by the Company's e-mail content scanner.

Policy shall be reviewed as and when necessary.

8. Incident Management (Policy & Procedures)

1. Introduction

The Company must protect this data using all means necessary by ensuring at all times that any incident which could cause damage to the Company's assets and reputation is prevented and/or minimized. There are many types of incidents which could affect security:

- A computer security incident is an event affecting adversely the processing of computer usage. This includes:
  - loss of confidentiality of information
  - compromise of integrity of information
  - denial of service
  - unauthorized access to systems
  - misuse of systems or information
  - theft and damage to systems
  - virus attacks
  - intrusion by humans
- Other incidents include:
  - Exposure of Uncollected print-outs
  - Misplaced or missing media
  - Inadvertently relaying passwords

Ensuring efficient reporting and management of security incidents will help reduce and in many cases, prevent incidents occurring. More detailed information on the type and scope of security incidents is provided in the Policy Statement section of this policy.

2. Purpose

Management of security incidents described in this policy requires the Company to have clear guidance, policies and procedures in place. Fostering a culture of proactive incident reporting and logging will help reduce the number of security incidents which often go unreported and unnoticed – sometimes, over a long period of time and often without resolution.

The purpose of this policy is to:

- Outline the types of security incidents
- Detail how incidents can and will be dealt with
- Identify responsibilities for reporting and dealing with incidents
- Detail procedures in place for reporting and processing of incidents
- Provide Guidance

3. Scope

This policy applies to:

- Company employees, elected members, and vendors
- All Company departments, personnel and systems (including software) dealing with the storing, retrieval and accessing of data

4. Policy Statement

The Company has a clear incident reporting mechanism in place which details the procedures for the identifying, reporting and recording of security incidents. By continually updating and informing Company employees, elected members, partner agencies, contractors and vendors of the importance of the identification, reporting and action required to address incidents, the Company can continue to be pro-active in addressing these incidents as and when they occur.

All Company employees, elected members, and vendors are required to report all incidents – including potential or suspected incidents, as soon as possible via the Company's Incident Reporting procedures.

The types of Incidents which this policy addresses include but is not limited to:

Computers left unlocked when unattended

Users of Company computer systems are continually reminded of the importance of locking their computers when not in use or when leaving computers unattended for any length of time. All Company employees, elected members, and vendors need to ensure they lock their computers appropriately - this must be done despite the fact that Company computers are configured to automatically lock after 5 minutes of idle time.

Discovery of an unlocked computer which is unattended must be reported via the Company's Incident Reporting procedures.

Password disclosures

Unique IDs and account passwords are used to allow an individual access to systems and data. It is imperative that individual passwords are not disclosed to others – regardless of trust. If an individual needs access to data or a system, they must go through the correct procedures for authorisation – initially through the individual's line manager. If anyone suspects that their or any other user's password has been disclosed whether intentionally, inadvertently or accidentally, the operation manager must be notified through the Company's Incident Reporting procedures. For more information, the Company Password policy is available on the intranet (Dnet) or via the Operation manager desk. Under no circumstances should an employee allow another employee to use their user account details after they have logged onto a system – even under supervision.

Virus warnings/alerts

All Desktop, laptop and tablet computers in use across the Company have Antivirus (including Anti-Spyware/Malware). For the most part, the interaction between the computer and antivirus software will go unnoticed by users of the computer. On occasion, an antivirus warning message may appear on the computer screen. The message may indicate that a virus has been detected which could cause loss, theft or damage to Company data. The warning message may indicate that the antivirus software may not be able to rectify the problem and so must be reported by the user to the system administrator as soon as possible.

Media loss

Use of portable media such as CD/DVD, DAT (magnetic tape), USB Flash sticks/HD drives for storing data requires the user to be fully aware of the responsibilities of using such devices. The use of PCs, laptops, tablets and many other portable devices increases the potential for data to be

exposed and vulnerable to unauthorised access. Any authorised user of a portable device who has misplaced or suspects damage, theft whether intentional or accidental of any portable media must report it immediately through the Company's Incident Reporting procedures.

Data loss/disclosure

The potential for data loss does not only apply to portable media it also applies to any data which is:

- Transmitted over a network and reaching an unintended, unauthorised -recipient (such as the use of e-mail to send sensitive data)
- Intercepted over the internet through non secure channels
- Posting of data on the internet whether accidental or intentional
- Published on the Company's website and identified as inaccurate or inappropriate (which must be reported)
- Conversationally – information disclosed during conversation
- Press or media – unauthorised disclosure by employees or an ill advised representative to the press or media
- Data which can no longer be located and is unaccounted for on an IT system
- Unlocked and uncollected print-outs from Multi-Function Devices (MFDs)
- Paper copies of data and information which can no longer be located
- Hard copies of information and data accessible from desks and unattended areas

All Company employees, elected members and vendors must act responsibly, professionally and be mindful of the importance of maintaining the security and integrity of Company data at all times.

Any loss of data and/or disclosure whether intentional or accidental must be reported immediately using the Company's Incident Reporting procedures

Personal information abuse

All person identifiable information – i.e. information which can identify an individual such as home address, bank account details etc… must not be disclosed, discussed or passed on to any person/s who is not in a position of authority to view, disclose or distribute such information.

Any abuse/misuse of such person identifiable information must be reported through the Company's Incident Reporting procedures.

Physical Security

Maintaining the physical security of offices and rooms where data is stored, maintained, viewed or accessed is of paramount importance. Rooms or offices which have been designated specifically as areas where secure information is located or stored must have a method of physically securing access to the room – e.g. a combination key lock mechanism. Lower floor/level windows could also provide access to the room/office and must also be securely locked – particularly when the room is left unattended. Rooms which have not been secured should not be used to store sensitive and personal information and data - concerns about any rooms/office which should be securely locked or access restricted must be reported to the Transformation Service via the Company's Incident Reporting procedures.

Continuing emphasis and re-enforcement of the Company's Secure Desk policy will further help to reduce the number of security incidents.

Logical Security / Access Controls

Controlling, managing and restricting access to the Authority's Network, Databases and applications is an essential part of Information Security. It is necessary to ensure that only authorized employees can gain access to information which is processed and maintained electronically.

Missing correspondence

Data or information which has been sent either electronically or physically which cannot be accounted for e.g. not arrived at the intended destination via physical post, sent electronically, sent for printing but no printed output retrieved etc… must be reported through the Company's Incident Reporting procedures.

Found correspondence/media

Data stored on any storage media or physically printed information which has been found in a place other than a secure location or a place where the security and integrity of the data/information could be compromised by unauthorised viewing and/or access e.g. unlocked printouts, discarded CD (media), must be reported through the Company's Incident Reporting procedures.

Loss or theft of IT/information

Data or information which can no longer be located or accounted for e.g. cannot be found in a location where it is expected to be, filing cabinet etc… or which is known/or suspected to have been stolen needs to be reported immediately through the Company's Incident Reporting procedures

1. Responsibilities

It is the responsibility for all Company employees, elected members, and vendors who undertake work for the Company, on or off the premises to be proactive in the reporting of security incidents. The Company's Incident Reporting procedures are in place to prevent and minimise the risk of damage to the integrity and security of Company data and information. It is also a responsibility of all individuals and handlers of Company data and information to ensure that all policies and procedures dealing with the security and integrity of information and data are followed.

2. Access of computer system

Restricted practice of unauthorised access to computer systems.

3. Breaches of Policy

Breaches of this policy and/or security incidents are incidents which could have, or have resulted in, loss or damage to Company assets, including IT equipment and information, or conduct which is in breach of the Company's security procedures and policies.

All Company employees, elected members, and vendors have a responsibility to report security incidents and breaches of this policy as quickly as possible through the Company's Incident Reporting Procedure. This obligation also extends to any external organisation contracted to support or access the Information Systems of the Company.

In the case of third party vendors, consultants or contractors non-compliance could result in the immediate removal of access to the system. If damage or compromise of the Company's ICT systems or network results from the non-compliance, the Company will consider legal action against the third party. The Company will take appropriate measures to remedy any breach of the policy through the relevant frameworks in place. In the case of an employee then the matter may be dealt with under the Company's disciplinary process or the relevant standards agencies in the case of elected members.

This Policy is referenced by other Company policies and guidelines. Copies of these policy statements are obtainable via the Company's Intranet (Dnet) or by request to the Transformation Service, as appropriate.

9. Incident Reporting and Management Procedure

Any incident, as described in the Policy, which needs reporting, will follow the process:

Overview

The Transformation Service will continually highlight the importance of incident reporting and will further encourage the use of the Company's Intranet where security breach incidents can be reported online. Where computer access to the Company network is not available, breaches can be reported via a telephone call to the administrator's Desk. Breaches can involve not only Information technology equipment but also data that is mishandled, lost or abused or any other incident which may cause a security concern or which may contravene the Company's Safe Haven Guidance and associated policies.

1.1 Incident Reporting

Any breach of the Incident Management Policy must be reported as soon as possible via the reporting procedure. Please note that the confidential reporting procedure will be observed by the provision of an alternative link which will provide a confidential reporting form.

There are various ways in which security incident breaches can be reported.

We recommend breaches to be recorded through the following:

- Using the Incident reporting form on intranet
- Via a Phone call to the System administrator Desk

There are other ways in which breaches can be recorded which include:

- E-mailing the Service Desk

- Visiting the Services

Reporting via the Service Desk

Security incidents and breaches can be reported by telephoning the administrator.

A Service Desk representative will log the details of the call in the call logging system based on the information given by the caller. Callers are advised to give as much information as possible and should be able to give similar details as required when completing the online form.

The Service Desk representative will log the call and any further progress or information about the incident will be dealt with by the Information Security Manager or nominated departmental representative.

Reporting via E-mail

Security breaches may be reported via e-mail to the administrator's desk however, wherever possible, confidential or personal identifiable information should not be contained in the e-mail e.g. logon passwords.

1.2 Incident Management

When an incident is reported and entered into the call logging system, an email is generated and sent to the system's administrator and also copied to the Information Security Manager. The Information Security Manager will then determine if the incident needs to be escalated to the appropriate pre-identified departmental representativeto deal with as soon as possible. Representatives looking into security breaches will be responsible for updating, amending and modifying the status of incidents in Service Manager.

All parties dealing with security incidents shall undertake to:

- analyse and establish the cause of the incident and take any necessary steps to prevent recurrence
- report to all affected parties and maintain communication and confidentiality throughout investigation of the incident
- identify problems caused as a result of the incident and to prevent or reduce further impact
- contact 3rd parties to resolve errors/faults in software and to liaise with the relevant Transformation Service and departmental personnel to ensure contractual agreements and legal requirements are maintained and to minimise potential disruption to other Company systems and services
- ensure all system logs and records are securely maintained and available to authorised personnel when required
- ensure only authorised personnel have access to systems and data
- ensure all documentation and notes are accurately maintained and recorded in Service Manager and made available to relevant authorised personnel

- ensure all authorised corrective and preventative measures are implemented and monitored for effectiveness

All incidents logged within Service Manager shall have all the details of the incident recorded – including any action/resolution, links or connections to other known incidents. Incidents which were initially resolved but have recurred will be reopened or a new call referencing the previous one will be created.

Monthly reports on incidents are prepared and send to management to facilitate the monitoring of the types, numbers, frequency and severity of incidents which will help to correct and prevent incidents recurring.

During the course of incident investigations, hardware, logs and records may be analysed by the Company's internal Audit function. Information and data may be gathered as evidence to support possible disciplinary or legal action. It is essential during the course of these investigations that confidentiality is maintained at all times.

The administrator is initially responsible for handling security incidents and will make a decision as to whether an incident needs to be "handed" over and dealt with (including closed) by departmental representatives where appropriate.

In this screen, the affected user is displayed along with the initial title and description of the incident. You will also notice there are 'drop down' sections which defines the incident further.

10. Business Continuity & Disaster Recovery Plan

1. Overview

In the e-age the information security is a very integral function for any business, more so in the broking industry. The broking business carries a lot of compliance and regulatory risk. Information and information systems are susceptible to a plethora of threats and vulnerabilities. The success of information security lies in protecting the confidentiality, integrity and availability of information.

For the purposes of this Plan a disaster is defined as any event (e.g. fire, explosion, serious flood, spillage/escape of hazardous substances) which requires evacuation of building and the attendance of the Emergency Services, There shall be substantial disruption to normal business in its aftermath, requiring mobilization of significant internal and external resources.

2. Scope

A Disaster Recovery Plan comprises of four parts:

2.1 Emergency Plan: This plan specifies the actions to be taken immediately after the disaster occurs. The following are the components of the emergency plan:

2.1.1 The plan shall show who is to be notified immediately when the disaster Occurs- management, police, fire departments, hospitals and so on

2.1.2 Actions to be undertaken, such as shutdown of equipment, removal of files and termination of power

2.1.3 Evacuation procedures shall be specified

2.1.4 Return and restart procedures shall be designated. In all cases the personnel responsible must be specified clearly.

2.2 Back-up Plan: This plan specifies the following information.

2.2.1 The type of back-up to be kept

2.2.2 The periodicity of the back-up

2.2.3 The procedure to be followed

2.2.4 The location of resources

2.2.5 The site where these resources can be assembled and operations restarted

2.2.6The personnel who are responsible for gathering back-up resources and restarting operations

2.2.7 The priorities to be assigned in recovering systems

2.2.8The time frame in which recovery of each system must be affected

2.3 Recovery Plan: The objective of this plan is to restore an organization's information systems to its full capabilities. The key focus is to identify a recovery committee who will be responsible for working out the modalities.
2.4 Test Plan: The emergency plan, back-up plan and recovery plan must be regularly tested using test plan.

3. Steps Involved in BCP/DRP
3.1.1 Initiate a business continuity plan work group and develop a BCP Strategy
3.1.2 Perform a risk assessment exercise to identify threats and exposures to each of the core business processes
3.1.3 Identify recovery strategies and identify recovery teams for each core business process
3.1.4 Test and validate the BCP/DRP plans.

4 BCP/DRP Team

4.1 The BCP/DRP team would consist of the following personnel

Name of the Person	Contact No.	Present Designation
Mr. ChanderPanwar	9810656902	I.T. Manager/App.Manager
Mr. Gaurav Kumar	8053770366	Tech Support Executive
Mr. Pawan Mishra	9717668564	App.Manager
Mr. Kuber Singh	9910325788	RMS Head
Ms. Bhawan Joshi	9990666924	Compliance Officer
Mr. Sanjay Sharma	9716363477	Accounts officer

5Basic Requirements for BCP/DRP:
5.1 The first step is the risk assessment that assists in finding the most important processes that support the business. The business activities shall be classified under 3 broad categories.

5.1.1 ***Category*** *A:* These include those business functions which cannot be performed unless they are replaced by identical capabilities. They cannot be replaced by manual methods. Tolerance to interruption is very low and therefore the cost of

interruption is very high. Examples:Secondary Market Trading activities, Depository Participant functions.

5.1.2 Category B: These are vital functions which can be done atthe end of the day. There is a higher tolerance to interruption and therefore the costs involved are lower than the critical functions. Examples: E-Mail Activities, Contract Notes in the back-office

***5.1.3 Category* C:** These functions are less crucial and can be managed for a brief period of time. Examples: Web-site, documents preparation.

5.2. Location for disaster recovery site: There are various factors involved in this decision like the distance from the main site, transportation and accommodation of the staff, seismic zone, political factors etc. We have DR site at:

IDC BKC TATA
Tata Communications
Limited, Plot No. C 36; G
Block ,BandraKurla,Complex, Bandra East;

6 Recovery Strategies

6.1 Hot Sites:

6.1.1 In this particular site there **would be complete** replication of data as that of the main active site. In the event of disruption, this site shall be fully configured and be ready to operate in several hours. The equipment, network and systems are fully compatible with the primary site. The only additional needs are staff, programs, data files and documentation.

6.1.2 There are two options available for making a hot site:

6.1.2.1 Create an own redundant hot site with the entire IT set-up same as the existing one

6.1.2.2 Use a third party hot-site.

6.2 ***Warm-Sites:*** These are partially configured, usually with network connections and equipments like disk drives, tape drives and controllers but without the main computer. The assumption behind the warm site is that the computer can usually be obtained quickly for emergency installation and since the computer is the most expensive unit such an arrangement is less costly than a hot site.

6.3Cold-Sites:Theyhave only the basic environment to operate an information processing facility reducingthe cost. Activation of the site may take several weeks.

7 Proposed Plan

The plan shall identify the teams with their assigned responsibilities in the event of a disaster/ incident. To implement the strategies that have been developed for business recovery and key decision making, IS and end- user personnel shall be identified. IT teams shall be made and they shall be assigned specific jobs. The teams may include:

7.1Incident response team:Thisteam shall receive information about every incident that can be considered as a threat to assets/processes.

7.2 Emergency action team: They are the first responders, designated fire wardens whose function is to deal with fires and other emergency response scenarios
7.3 Damage Assessment team: They assess the extent of damage following the disaster. The team shall include staff expert in systems and networks and trained in safety regulations and procedures
7.4 Off-site storage team: responsible for obtaining, packaging and shipping media and records to the recovery facility
7.5 Applications team: Travels to the recovery site and restores user packs and applications program on the backup system
7.6 Security *Team:* Continually monitors the security of the system and communication links, resolves any security conflicts that impede the expeditious recovery of the system
7.7 Emergency *operations team:* Consists of shift operators and shift supervisors who will reside at the systems recovery site and manage systems operations during the entirety of the disaster
7.8 **Network recovery team:** Responsible for rerouting wide-area voice and data communications traffic, reestablishing host network control and access at the system recovery site
7.9Communications team: Travels to the recovery site where they work in conjunction with the remote network recovery team to establish a user/system network
7.10 Data preparation and records team: Working from terminals that connect to the user recovery site and update the applications database
7.11 Administrative support **team:** Provides clerical support to the other teams and serves as a message centrefor the user recovery site
7.12 Legal affairs team:Responsible for handling the legal issues arising for various reasons due to any incident.
7.13 Recovery test team:Responsible for testing of various plans developed We have formed the BCP/DRP team and have specified the functions for the team members. The following matrix explains the nature of functions assigned to the staff members and the support team of the vendors in the event of a disruption or disaster at the server station:

11. Anti-Money Laundering Policy (PMLA)

Background

The Prevention of Money Laundering Act, 2002 (PMLA) has been brought into force with effect from 1st July, 2005. As per the provision of the Act all the intermediaries registered under section 12 of the SEBI Act, 1992 shall have to maintain a record of all the transactions, the nature and value of which has been prescribed in the rules under PMLA. SEBI has also issued a circular no: ISD/QR/RR/AML/1/06 on Jan 18, 2006 to all intermediaries registered with SEBI under section 12 of the SEBI Act providing guidelines on Anti Money Laundering Standards.

As per the provisions of the Act senior management of the company are fully committed to establish appropriate policies and procedures for prevention of money laundering and terrorist financing and ensuring the effectiveness and compliance with all relevant legal and regulatory requirement. They have formulated a system for identifying, monitoring and reporting and reporting to law enforcement authorities about suspected transactions occurred for Money laundering and terrorist financing.

The Government of India has serious concerns over money laundering activities which are not only illegal but anti-national as well. As a market participant it is evident that strict and vigilant tracking of all transactions of suspicious nature required.

Accordingly the Company has laid down following policy guidelines:

Policy Statement

Open Futures& Commodities Pvt. Ltd. is fully committed to combat any effort of laundering money earned through drug trafficking, terrorism and any other means of organized and serious crimes by any individual or entity. Towards this "**Open Futures Group Companies"** has put in place all such processes and procedures of internal control aimed at preventing and impeding any attempt of money laundering and terrorist financing using the services offered by its group companies.

Appointment of Principal Officer:

As per Circular No. MCX/COMP/488/2009 dated November 27, 2009, **Open Futures & Commodities Pvt. Ltd**. has designated**Ms. Bhawna Joshi** as Principal Officer, who will be responsible for monitoring and reporting of all transactions and sharing of information as required under the law. The name, designation and address (including e-mail address) of the 'Principal Officer' has been intimated to the Office of the Director-FIU, 6th Floor, Hotel Samrat, Chanakyapuri, New Delhi – 110021. (Refer Circular No. MCX/COMP/488/2009 dated November 27, 2009)

Purpose & Scope of the policy:

As a Financial Market Intermediary (which includes a stock-broker, sub-broker) we need to maintain a record of all the transactions; the nature and value of which has been prescribed in the Rules under the PMLA. Accordingly all the back office and trading staff is instructed is instructed to observe the following safeguards:

1. No Cash transactions for trading in securities shall be allowed from any client in the normal course of business.
2. Maintain a record of all the transactions; the nature and value of which has been prescribed in the Rules notified under the PMLA. Such transactions include:

- Cash transactions of the value of more than Rs 10 lakhs or its equivalent in foreign currency.
- All series of cash transactions integrally connected to each other which have been valued below Rs 10 lakhs or its equivalent in foreign currency where such series of transactions take place within one calendar month.
- All suspicious transactions whether or not made in cash.

3. Frequent off Market transfers from one BO account to another shall be scrutinized and asked for. In absence of valid reason case or found suspicious, it shall be brought to the notice of Principal Officer.

4. Trading beyond ones declared income: The turnover of the clients should be according to their declared means of income. Any abnormal increase in client's turnover shall be reported to Principal Officer. The Back Office staff should take due care in updating the clients' financial details and shall periodically review the same.

Policies &Procedures :

Customer Due Diligence :

The 'Know your Client' (KYC) Policy : -

A. **While establishing the intermediary – client relationship**

No account shall be opened unless all the KYC Norms as prescribed from time to time by the SEBI / Exchanges are duly complied with, all the information as required to be filled in the KYC form (including financial information, occupation details and employment details) is actually filled in and the documentary evidence in support of the same is made available by the client. Moreover all the supporting documents should be verified with originals and client should sign the KYC & MCA in presence of our own staff and the client should be introduced by an existing clients or the known reference.

The information provided by the client should be checked though independent source namely.

Pan No must be verified from Income Tax Web Site

Address must be verified by sending Welcome Letter / Qtly Statement of Account, and in case any document returned undelivered the client should be asked to provide his new address proof before doing any further transaction.

We must exercise additional due diligence in case of the **Clients of Special Category** which include but not limited to :-

i. Non resident clients
ii. High networth clients (i.e the clients having networth exceeding 20 Lakhs and doing the intra day trading volume of more than 2 Crore and daily delivery volume more than Rs 20 Lakhs)
iii. Trust, Charities, NGOs and organizations receiving donations
iv. Companies having close family shareholdings or beneficial ownership
v. Politically exposed persons (PEP) of foreign origin
vi. Current / Former Head of State, Current or Former Senior High profile politicians and connected persons (immediate family, Close advisors and companies in which such individuals have interest or significant influence)
vii. Companies offering foreign exchange offerings
viii. Clients in high risk countries (where existence / effectiveness of money laundering controls is suspect, where there is unusual banking secrecy, Countries active in narcotics production, Countries where corruption (as per Transparency International Corruption Perception Index) is highly prevalent, Countries against which government sanctions are applied, Countries reputed to be any of the following – Havens / sponsors of international terrorism, offshore financial centres, tax havens, countries where fraud is highly prevalent.
ix. Non face to face clients
x. Clients with dubious reputation as per public information available etc.
xi. Such Other persons who as per our independent judgment may be classified as CSC.

In case we have reasons to believe that any of our existing / potential customer is a politically exposed person (PEP) we must exercise due diligence, to ascertain whether the customer is a politically exposed person (PEP), which would include seeking additional information from

clients and accessing publicly available information etc.

The dealing staff must obtain senior management`s prior approval for establishing business relationships with Politically Exposed Persons. In case an existing customer is subsequently found to be, or subsequently becomes a PEP, dealing staff must obtain senior management`s approval to continue the business relationship.

We must take reasonable measures to verify source of funds of clients identified as PEP.

The client should be identified by using reliable sources including documents / information and we should obtain adequate information to satisfactorily establish the identity of each new client and the purpose of the intended nature of the relationship.
The information should be adequate enough to satisfy competent authorities (regulatory / enforcement authorities) in future that due diligence was observed by the intermediary in compliance with the Guidelines. Each original documents should be seen prior to acceptance of a copy.

Failure by prospective client to provide satisfactory evidence of identity should be noted and reported to the higher authority.

While accepting a client the underlying objective should be to follow the requirements enshrined in the PML Act, 2002 SEBI Act, 1992 and Regulations, directives and circulars issued there under so that we are aware of the clients on whose behalf we are dealing.

c. **While carrying out transactions for the client**

RMS department should monitor the trading activity of the client and exercise due diligence to ensure that the trading activity of the client is not disproportionate to the financial status and the track record of the client.
Payments department should ensure that payment received form the client is being received in time and through the bank account the details of which are given by the client in KYC form and the payment through cash / bearer demand drafts should not be entertained.

B. **<u>Policy for acceptance of clients:</u>**

The following safeguards are to be followed while accepting the clients:
a. No account is opened in a fictitious / benami name or on an anonymous basis. To ensure this we must insist the client to fill up all the necessary details in the KYC form in our presence and obtain all the necessary documentary evidence in support of the information filled in KYC. We must verify all the documents submitted in support of information filled in the KYC form with the originals and ***in-person verification should be done by our own staff. Moreover new client should either be introduced by an existing customer or by the senior official of the company***. In case we have any doubt that in-complete / fictitious information is submitted by the client, we must ask for such additional information so as to

satisfy ourselves about the genuineness of the client and the information of the client before accepting his registration.

b. Factors of risk perception of the client :-

Particulars	Risk Perception
Factors of Risk Perception having regard to :	
Client`s Location (Registered / Correspondence/ other address)	
- Face to Face clients of Delhi NCR	Low Risk
- Face to Face clients of other than Delhi NCR	Low Risk
- Client Introduced by existing Face to Face Clients	Low Risk
- Client Introduced by other Existing Clients	Medium Risk
- Direct Clients of Delhi NCR	Medium Risk
- Direct Clients of other than Delhi NCR	High Risk
- Non resident Clients	High Risk
Nature of Business Activity, Trading Turnover etc	
-Retail clients (average daily turnover <Rs 10 Lakhs or net settlement obligation <Rs 2 Lakhs)	Low Risk
- Retail clients (average daily turnover <Rs 25 Lakhs or net settlement obligation <Rs 5 Lakhs)	Medium Risk
- HNI Clients (average daily turnover >Rs 25 Lakhs or net settlement obligation >Rs 5 Lakhs)	High Risk
Manner of Making Payment	
- Regular payment through A/c payee cheque from the Bank A/c already mapped with us	Low Risk
- Payment through A/c payee cheque from the Bank A/c other than one already mapped with us	Medium Risk
- Payment through Banker`s Cheque / Demand Draft / Cash	High Risk
Client of Special Categories as defined under Para A (a) of these Guidelines	Very High Risk

c. Ensure that no account is opened where we unable to apply appropriate clients due diligence measures / KYC policies. This shall be applicable in cases where it is not possible to ascertain the identity of the client or information provided by the client is suspected to be non genuine or perceived non co-operation of the client in providing full and complete information. We should not continue to do business with such a person and file a suspicious activity report. We should also evaluate whether there is suspicious trading in the account and whether there is a need to freeze or close the account.

Policy for *Recruitment of personnel*

The HR Department is instructed to cross check all the references and should take adequate safeguards to establish the authenticity and genuineness of the persons before recruiting. The department should obtain the following documents:

1. Photographs
2. Proof of address
3. Identity proof
4. Proof of Educational Qualification
5. References

Retention of records

Records pertaining to active clients and staff details collected for recruitment shall be kept safely.

Information to be maintained

Company will maintain and preserve the following information in respect of transactions referred to in Rule 3 of PMLA Rules for the period of 10 years.

I. Client Registration Forms
II. Contract Note
III. the nature of the transactions;
IV. the amount of the transaction and the currency in which it denominated;
V. the date on which the transaction was conducted; and
VI. the parties to the transaction.

Employees' Training

Company adopted an ongoing employee training program so that the members of the staff are adequately trained in AML and CFT procedures.

Training requirements have specific focuses for frontline staff, back office staff, compliance staff, risk management staff and staff dealing with new customers. It is crucial that all those concerned fully understand the rationale behind these guidelines, obligations and requirements, implement them consistently and are sensitive to the risks of their systems being misused by unscrupulous elements.

Investors Education

Implementation of AML/CFT measures requires back office and trading staff to demand certain information from investors which may be of personal nature or which have hitherto never been called for. Such information can include documents evidencing source of funds/income tax returns/bank records etc. This can sometimes lead to raising of questions by the customer with regard to the motive and purpose of collecting such information. There is, therefore, a need for the back office and trading staff to sensitize their customers about these requirements as the ones emanating from AML and CFT framework. The back office and trading staff should prepare specific literature/ pamphlets etc. so as to educate the customer of the objectives of the AML/CFT program me.

Reporting to FIU

As per our observations if any transaction of suspicious nature is identified it must be brought to the notice of the Principal Officer who will submit report to the FIU if required.

Above said policies are reviewed by us on regular basis to keep it updated as per the various amendments in the PMLA rules.

SURVEILLANCE POLICY

A. Background

We along with our Employees are the first touch point in the securities market/commodities for investors and are expected to have reasonably fair understanding about their client(s) and its trading activity. Thus, Exchanges/regulators have entrusted on us the first level of the responsibility to ensure that neither us nor our client(s) are misusing the trading system by indulging in manipulation or any other illegal activities which can cause risk to the integrity of the market and distorts the equilibrium of the market.

Objectives of framing a surveillance policy covering

1.1. Alerts to be generated.
1.2. Threshold limits and the rationale for the same.
1.3. Review process.
1.4. Time frame for disposition of alerts and if there is any delay in disposition, reason for the same should be documented.
1.5. Suspicious/Manipulative activity identification and reporting process.
1.6. Record Maintenance.

B. Surveillance framework

It is mandatory under the exchange/regulatory directives to have in place appropriate Surveillance Policies and Systems to detect, monitor and analyze transactions. For the above we have to co-relate the transaction data with their clients' information/data and. Detect suspicious/manipulative transactions is an ongoing continuous process with analysis of trades and transactions and carrying out Client Due Diligence (CDD) on a continuous basis.

In-order to implement the exchange directives, they have provided us alerts which have to be generated by us. In addition to this we have also developed in-house surveillance software. The details of both these have been enumerated below:

I. EXCHANGE ALERTS

1. **Unusual trading activity:** Client(s)/Group of Client(s) who have been dealing in smallquantities/value suddenly significantly increase their activity over a period of time say fortnight/month/quarter and this increases by certain threshold limit of more than 50% as compared to the earlier period of same duration, we

have review and conduct a analysis on parameters such as;

1. Whether such volume is justified give the background of the client and his past trading activity.
2. Amount of funds that was brought in by the Client(s)/Group of Client(s) for the purchases made during the period.
3. Whether such inflow of funds is in line with the financial status of the client.
4. Whether the transactions of such Client(s)/Group of Client(s) are contributing to concentration or impacting the price and or volumes.

2. **Sudden trading activity in dormant accounts-**An inactive client resumes tradingstarts/resumes trading and additionally the client start trading in illiquid stocks or low market capitalized scrips or enters into huge transactions not to commensurate with the financial strength of the client, we have to review and examine the following;

1. Reasons for trading in such scrips/contracts/commodity.
2. Whether there is any concerted attempt by a Client(s)/Group of Client(s) to impact the prices.
3. Whether there is any concerted attempt by a Client(s)/Group of Client(s) to indulge in movement of profit/loss from one client to another account.

3. **Clients/Group of Client(s), deal in common scrips/contracts/commodity contributing significant to the volume of the scrip/contract at the Trading Member level and at the stock exchange level.** We need to review and examine the following;
   1. Reasons for trading in such scrips/contracts/commdity.
   2. Whether there is any concerted attempt by to impact the prices.
   3. Whether there is any concerted attempt to indulge in movement of profit/loss from one client to another.

4. **Activity of Client(s)/Group of Client(s) is concentrated in a few illiquid scrips/contracts/commodity or there is a sudden activity by Client(s)/Group of Client(s) in illiquid securities/contracts manifested in terms of volume as compared to the volume of the exchange or that of the Trading Member.** We need to review and examine the following;
   1. Reasons for trading in such scrips/contracts/commdity.
   2. Whether there is any concerted attempt to impact the prices.
   3. Whether there is any concerted attempt to indulge in movement of profit/loss from one client to another.

5. **Client(s)/Group of Client(s) dealing in scrip in quantity of one share or trade in minimum lot size.** We need to review and examine the following
   1. Reasons for such trading behavior.
   2. Trading pattern and repeated instances.

6. **In accordance to the list of illiquid scrips/contracts/commodity provided by exchanges**, we need toreview and examine the following;

1. Whether there trading is sudden trading
2. Whether there is any concerted attempt to impact the prices of such scrips/contracts/commodity.
3. Whether there is any concerted attempt to indulge in movement of profit/loss from one client to another.
4. Probable matching of transactions with another client.
5. Apparent loss booking transactions in illiquid contract/securities/commodity.
6. Whether the transactions of are contributing to concentration or impacting the price.

7. Circular Trading:

6. Continuous trading of client/group of clients in particular scrip over a period of time.
7. Client/group of clients contributing significant volume (broker and exchange level) in a particular scrip – especially illiquid scrip and /or illiquid contracts
8. Possible matching of trades with a specific group of clients (like same trade number on both buy and sell side of a member and/or immediate execution of order in illiquid scrip etc.)
9. Possible reversal of trades with the same group of clients (like same trade number on both buy and sell side of a member and/or immediate execution of order in illiquid scrip)

8. Pump and Dump:

1. Activity concentrated in illiquid scrips/contracts/commodities.
2. Sudden activity in illiquid securities/contracts/commodity.
3. Percentage of activity to total market in the scrip/contract/commodities is high.
4. Trades being executed at prices significantly away from the market and later on squaring off to earn significant profits.

9. Wash Sales or Reversal of Trades:

1. Same Client) on both sides of the transaction. (i.e. same trade number on both the buy and sell side with us)
2. Reversal of transactions by same Client(s) or within same Group of Client(s) at significantly different trade prices within a short period of time says 3-4 days.
3. One client makes significant profit and other suffers a loss or apparent loss booking transactions in illiquid contract/securities including options

10. Front Running:

7. Trading, by Client employees, ahead of large buy/sell transactions and subsequent square off has to be identified and such transactions have to be reviewed for determining front running
8. There is a consistent pattern of Client employees trading ahead of large buy/sell transactions.

11. Concentrated position in the Open Interest/high turnover concentration:

1. Client having significant position in the total open interest of a particular scrip.
2. Client not reducing/closing their positions in spite of the scrip being in ban period.
3. Client activity accounts for a significant percentage of the total trading in the contract/securities at member and exchange level.
4. Monitor the trading pattern of Client(s) who have Open Interest positions/concentration greater than equal to the thresholds prescribed.

12. Order book spoofing i.e. large orders away from market :

1. Consistent placement of large orders significantly away from the market with low trade to order trade ratio or canceling orders within seconds after placing them thereby creating a false impression of depth in a particular scrip/contract
2. Repeated pattern of placement of large buy orders which are away from the market price and simultaneous placement of sell orders to benefit from price rise or vice-versa.

II. OFFLINE IN-HOUSE ALERTS

1) **Report on Delivery above Rs.500000 & TO above Rs.2500000 – all segments of equities and commodities** Placement of large orders with the delivery turnover contributing invalue terms above Rs. 50,000 and trading turnover in terms of value above Rs.2,50,000/-
for all segments are generated.

1. In case if the name of any new client appears in this report and / or the name of the client comes again in the report after a period of 15 days to one month, then compliance team informs about the said trade details to the RMS team,
2. Thereafter RMS team does the trade/ledger confirmation with the end client and accordingly updates the compliance team.

2) **CASH Excess Volume (more than 5% of market volume) (equity segment and commodity segment)** Trades inequity segment contributing to more than 5% of the exchange volume are generated.

1. The records so generated are analysed vis-a vis exchange volume, repeated days of the trading and price volatility, company financials etc.
2. In case of any repeated days of trading, contributing to significant exchange volumes and or price volatility or concentrated trading among selective group of client is observed, then in such instances after analysis appropriate steps are taken.

3. **Illiquid scrip (equity segment)** Trades in equity segment for the illiquid scrips (which
have been identified as illiquid by exchange) are generated.

1. The records so generated are compared visa vis. exchange volumes, repeated days of trading, price volatility in the scrip.
2. Additionally the financials of the company are also analyzed to ascertain whether the trading volumes and price movements are justified.
3. In case any trading is found to be abnormal, initial alerts are sent to the branches. If repeated, after proper verification and analysis the scrip may also is blocked from further trading.

3) **F&O Profit/Loss & Futures Rate Fluctuation (equity derivatives)**Trades in equityderivatives for the above referred parameter which are generated in case of clients
executing trades at price above 20% of the previous closing price and or incurring huge profits or losses are generated.

1. For the records generated under this alert are evaluated in case of any un-usual pattern clarification from the client/or branch is sought.

4) **F&O Excess Volume (more than 5% of market volume) (equity and commodity derivatives)**Trades in derivatives and commodity derivative are generated in trades aremore than 5% of market volumes

1. For the records generated under this alert are evaluated visa-vis the strike price, maturity date of the contract, type of derivative contract, underlying etc are analyzed and evaluated.
2. In case if the name of any new client appears in this report and / or the name of the client comes again in the report after a period of 15 days to one month, then compliance team informs about the said trade details to the RMS team.
3. Thereafter RMS team does the trade/ledger confirmation with the end client and accordingly updates the compliance team.

5) **Matching of Trades – all segments (equities and commodities)**The trades which getmatched (applicable for all segments) at member level and or client level are generated under this alert.

1. The records so generated, comparison is done to ascertain whether they have been carried out from the same trading terminal or same location or for group of same family codes.
2. In case of illiquid scrip/contracts or significant volumes or price volatility observed, explanation is sought and or warning is issued to the client.

III. ONLINE IN-HOUSE ALERTS

The following are the various alerts, wherein the records coming under these alerts are analyzed with the financials of the company, repetitive nature of the instances, volumes and or price volatility. These alerts are observed by the RMS on real time basis and in case of any suspicious nature, appropriate reasons are sought from the branch/franchisee/clients. We have summarized the online alerts which are being monitored as on date:

1) **Module of Online Trade Matching Popup:** In this module all the trades that get matchedcan be viewed and thereafter further verification and/or analysis is done.

2) **Module of Online Delivery Tracker:** This report provide the trades of the clients whotake delivery above Rs. 5 lacs in value terms or all delivery above 10,000 in quantity terms (this limit is modified on time to time basis.

3) **Module on Online Ban Scrip Position Tracker:** This report provides the records in caseany client takes position in "Ban" security, then we can come to know via this pop up that position is open and may attract penalty in case position is carried further.

4) **Module on Unregistered/Inactive Client Trade:** This report shows that in case any clientis inactive as per our backoffice software or not registered, in spite of which trade is done the details can be ascertained via trading terminal and can be restricted from further trading and to complete the reactivation/registration process as the case may be.

5) **Module on Spurt in volume:** This reports provide the records of the trades in whichthere is any sudden increase in volume in comparison with 2 weeks average exchange volume.

6) **Matching of Trades (in commodities):** The trades which get matched at member leveland or client level are generated under this alert. The records so generated, comparison is done to ascertain whether they have been carried out from the same trading terminal or same location or for group of same family codes.

IV. ADDITIONAL MONITORING

1. Not allowing trades of entities which are banned by SEBI/Exchange/other regulators. This database is verified by the KYC team before client account is activated.

2. Trading is allowed to commence only after execution of the client registration form and all the mandatory Unique Client Code (UCC) parameters such as Name, Address, PAN No. etc., have been uploaded by us to the Exchange portal.

3. Likewsie, demat account numbers are provided to the demat account holders only after obtaining the Client registration forms and activating the same into the DP system.

4. Clients who have debit balance in their ledgers continuously for a certain period of time or who default in making payment/delivery. This is monitored by our RMS team who dedicated does follow up with the clients/branches/AP's and also restricts from further trading.

5. Bulk deals have been disclosed/reported; illiquid scrips/contract or derivatives scrips which are in ban period. Trading activity in such scrips may be analyzed for Client.

We need to correlate the transactional alerts with the information of client(s) available with them. The correlation of alerts with information of Client(s)/Group of Client(s) would help Trading Members to identify, mitigate and manage such transactions as well as minimizing business risk.

C. <u>Analysis</u>

In order to analyze the trading activity of the Client scrips identified based on above alerts, we can do the following:-

1. Shortlist Client for further analysis.

2. Seek explanation from such identified Client

3. Seek documentary evidence such as bank statement/demat transaction statements of last 6 months to 12 months period, to satisfy itself.

4. On the basis of information received from the client and after proper evaluation and analysis, we decide our steps for suspending code and or the scrip from further trading.

D. <u>Reporting</u>

All action/analysis with respect the alerts generated should be completed within a reasonable time frame

The surveillance policy of the Trading Member to be approved by the Board of Directors

A daily reporting of the alerts to the designated director and principal officer / a quarterly MIS to the Board of Directors if there are alerts as to the number of alerts received, disposed off during the quarter and pending at the end of the quarter and the. Reasons for pendency should be discussed and appropriate action taken for disposing of the alerts.

The surveillance process to be conducted under overall supervision of its Compliance Officer/Principal Officer.

Principal Officer under the PMLA directives/ Compliance Officer of the Company and their team would be to be responsible for all surveillance activities carried out for the record maintenance and reporting of such activities under the supervision of the Designated Director.

Internal auditor shall review the surveillance 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.

This policy would be made available to the internal auditors and regulators during the course of audits or as and when demanded.

Certain few things we can implement provided the concerned departments monitor and keep track

1. **Frequent instances of payment by Client(s)/Group of Client(s) in the form of cash equivalents like Demand Draft, Pay order etc. to be monitored for**

2. **When home or business telephone number has been disconnected or there is no such number when an attempt is made to contact client or documents sent at its email/home/business address returned undelivered.**

3. **Having multiple accounts with the Trading Member and using different trading accounts alternatively.**

4. **Client frequently changing bank/ demat account.**

Error Account Policy

1. The modification to the client code is to be done only in exceptional cases and not as a routine one.
2. The reason for modification has to be ascertained and analyzed and genuineness is to be established and alsoit's impact on the clients should be studied before the modification. If voice recording is in practice, the same is being studied.

3. Normally as a principle, we are permitted to change client codes of non-institutional clients only for the following objective criteria;

   a. Error due to communication and/or punching or typing such that the original client code/name and the modified client code/name are similar to each other.
   b. Modification within relatives (Relative for this purpose would mean 'Relative' as defined under sec. 6 the Companies Act, 1956).

4. For easy identification of error account, we register a fresh client code as "ERROR" in the UCC database of the Exchange for the account which is classified as error account.

5. We will inform the Exchange (through BEFS), by end of day, the reasons for modification of client codes of non-institutional trades based on the aforesaid objective criteria.

6. Therefore it is imperative that the issue should be reported to the senior level Manager/Director/Proprietor and only with his approval, the modification should be carried after being satisfied that it is genuine, the same is required to be done to protect the interests of the client.

7. Hence the facility to modify the client codes should be available only at the Corporate Manager level and should not be given to the branches/franchise/sub-brokers.

8. Training program should be conducted to all the Dealers and they should be explained how code modifications can be misused and what steps should be taken to avoid the same. It also should be explained that code modifications should not be encouraged to the clients except for cases like 'punching errors'/'typing errors'.

PRE - FUNDED POLICY

It's a Policy of the Company for the acceptance of Prefunded Instruments. This policy is Subject to the rules and regulations of the Exchange from time to time.

Open Futures *does not take pre funded instruments from the clients but there is a policy for exceptional cases.*

Title: Acceptance of Prefunded Instrument for trades on Exchanges. Coverage: Head office only.

Scope: Acceptance of Prefunded Instruments like Demand Draft/Payorder/Bank Guarantees from a client against Payin Obligation/ Margin. Procedures: The Prefunded Instruments must be accepted only in following special circumstances;

1) If there are Bank Holidays on the following day.
2) If the client does not have an account in the bank in which the company has accounts.
3) If the client wants to create a position immediately and has no other way of transferring funds.
4) If the Bank account of the client is in a cooperative bank, which may take some time for the cheque to be cleared.
5) If the company Bank accounts clearing branch is not available in the city/village where the client has his bank account.

The Objective of this policy is to minimize the frequency of acceptance of Prefunded Instrument, especially Demand Draft where there is a difficultyin tracking the correct source of Issuance.

Permissible Limits: The Prefunded Instruments must be accepted only in cases mentioned above and not otherwise. Approval for acceptance must be taken by either of the executive Directors or the Managing Director and only then credit should be given.

CONFLICT OF INTEREST POLICY

Introduction

SEBI vide its circular no. CIR/MIRSD/5/2013 dated August 27, 2013 issued a General Guidelines for dealing with Conflicts of Interest of Intermediaries, Recognised Stock Exchanges, Recognised Clearing Corporations, Depositories and their Associated Persons in Securities Market. SEBI decided to put in place comprehensive guidelines to collectively cover such entities and their associated persons, for elimination / avoidance of their conflict of interest and educating the Associated Persons as defined in Securities and Exchange Board of India (Certification of Associated Persons in the Securities Markets) Regulations, 2007 for the compliance of the guidelines.

SEBI advised to lay down, with active involvement of senior management, policies and internal procedures to identify and avoid or to deal or manage actual or potential conflict of interest, develop an internal code of conduct governing operations and formulate standards of appropriate conduct in the performance of their activities, and ensure to communicate such policies, procedures and code to all concerned;

SEBI guidelines intends Intermediaries and their Associated Persons to comply with thefollowing –

- High standards of integrity in the conduct of business;
- Fair treatment of clients and no discrimination amongst them;
- Avoidance of conflict of personal interest with the client and primacy of clients' interest;
- Appropriate disclosure to the clients of possible source or potential areas of conflict of interest;
- Reducing the opportunities for conflict through prescriptive measures;
-Appropriate restrictions on transactions in securities while handling a mandate of issuer or client;
- Not to deal in securities while in possession of material non published information;
- Not to communicate the material non published information
- Not to manipulate the demand for, or supply of, or to influence prices of, securities.
- Not to have an incentive structure that encourages sale of products not suiting the risk profileof the clients;
- Not to share client information for the personal interest;

We**Open Futures& Commodities Pvt. Ltd.** hereby provide the policy we maintain in order to manage conflict of interest in respect of the duties we owe to our clients.

This Policy is not intended to, and does not create third party rights or duties that would not already exist if the Policy had not been made available.

Purpose

The purpose of this document is to set out the Company's approach in identifying and managing conflict of interest which may arise during the course of its business activities. The Policy applies to all its directors, employees, any persons directly or indirectly linked to the Company (hereinafter called "related persons") and refers to all interactions with clients.
The aim of our Policy is to identify and prevent conflict of interest which may arise between the Company and its clients or between one client and another. Accordingly, we have adopted a conflict of interest policy setting out the procedures, practices and controls in place to achieve this.

The process entails the following actions:

I. Identification of conflict of interest situations
II. Management of conflict of interest situations
III. Disclosure of conflict of interest and record keeping

Identification of Conflict of Interest situations

For the purposes of identifying the types of conflict of interest that arise in the course of providing investment and ancillary services or a combination thereof and whose existence may damage the interest of a client, the Company takes into account, whether the Company or a relevant person, is in any of the following situations, as a result of providing investment or ancillary services or investment activities or otherwise:

1 The Company or relevant person is likely to make a financial gain, or avoid a financial loss, at the expense of the client;
2 The Company or a relevant person 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;
3 The Company or relevant person has a financial or other incentive to favor the interest of another client or group of clients over the interests of the client;
4 The Company or a relevant person carries the same business with the client;
5 The Company or a relevant person receives or will receive from a person other than the client an inducement in relation to a service provided to the client, in the form of money, goods or services, other than the standard commission or fee for that service.

Conflict of Interest situation can be divided into two categories:
(a) Conflict of interest which might arise between Clients and the Company (management, employees, tied agents etc.) and
(b) Between the clients themselves

Taking into consideration the services the Company offers, potential circumstances giving rise to Conflict of Interest may be related to the Reception and transmission of orders, Execution of orders, Dealing on own account and/or Ancillary services.

The paragraph below specifies some of the major sources of potential conflict of interest, which may arise:
1 In the area of Investment Research and in particular, from the Company's own interest in the sales of financial instrument(s)
2 From payments (e.g. commissions) received from or made to third parties in connection with investment services provided to them
3 From performance – related remuneration of employees and agents
4 From other business activities of the Company, especially, from the Company's interest in profits from trading on its own account
5 From personal relations of employees or members of the Company's Board of Directors or parties related to such persons

Management of Conflict of Interest situations

The Company has set up internal policies and has an in-house Compliance Department that is responsible for identifying and managing potential conflict of interest. The above mentioned Department also updates the relevant internal procedures and ensures compliance with such procedures.

The Company maintains and operates effective organizational and administrative procedures to manage the identified conflict of interest. The Company also undertakes ongoing monitoring of business activities to ensure that internal controls are appropriate.

In general, the procedures and controls that the Company follows regarding conflict of interest include the following measures:

(a) Effective procedures to prevent or control the exchange of information between relevant persons engaged in activities involving risk of conflict of interest where the exchange of that information may harm the interests of one or more clients;
(b) The separate supervision of relevant persons whose principal functions involve carrying out activities on behalf of, or providing services to, clients whose interests may conflict, or who otherwise represent different interests that may conflict, including those of the Company;
(c) The removal of any direct link between the remuneration of relevant persons principally engaged in one activity and the remuneration of, or revenues generated by, different relevant persons principally engaged in another activity, where conflict of interests may arise in relation to those activities;
(d) Measures to prevent or limit any person from exercising inappropriate influence over the way in which a relevant person carries out investment or ancillary services or activities;
(e) Measures to prevent or control the simultaneous or sequential involvement of a relevant person in separate investment or ancillary services or activities where such involvement may impair the proper management of conflict of interest.

Some of these policies and procedures established to prevent Conflict of Interest are shown below:

- A 'need to know' policy governing the dissemination of confidential or inside information within the Group
- Chinese walls restricting the flow of confidential and inside information within the company and physical separation of departments
- Procedures governing access to electronic data
- Segregation of duties that may give rise to conflict of interest if carried out by the same individual
- Personal account dealing requirements applicable to relevant persons in relation to their own investments
- A gifts and inducements log registering the solicitation, offer or receipt of certain benefits

- The prohibition of external business interests conflicting with our interests as far as the Group's officers and employees are concerned, unless board approval is provided.
- A policy designed to limit the conflict of interest arising from the giving and receiving of inducements
- Establishment of an in-house Compliance Department to monitor and report on the above to the Company's Board of Directors
- Appointment of an internal auditor to ensure that appropriate systems and controls are maintained and report to the Company's Board of Directors
- Establishment of the four-eyes principle in supervising the Company's activities

Disclosure of conflict of interest and record keeping

Where the organizational and administrative arrangements described above are not sufficient to ensure with reasonable confidence that the risks of damage of the client's interests will be prevented, the Company clearly discloses the general nature and/or source of conflict of interest to the Client before undertaking business on his behalf.

Disclosure to Clients is done in sufficient detail to enable the Clients to make an informed decision about the investment and ancillary service in the context of which the conflict arises.

If the Company, however, does not believe that disclosure is appropriate to manage the conflict, it may choose not to proceed with the transaction or matter giving rise to the conflict.

The Company reserves the right to review and/or amend its Policy and arrangements whenever this is deemed to be appropriate. Further information about this summary document is available upon request.

Should you have a question about conflicts of interest please direct your questions to our Compliance Department: bhawnajoshi@openfutures.in

Inactive Client Account Policy

This policy defines the treatment of Dormant/Inactive accounts of the clients maintained with the company **(Open Futures & Commodities Pvt. Ltd.).**

Definition of Dormant / Inactive accounts

In order to protect the account of customer, Open Futures will deactivate the trading accounts of the client, which are identified as "Dormant" and report them as inactive in UCC.

In case of trading account the term dormant/Inactive account refers to such account where no transaction have been carried out since last 1 (Year) from the account opening date or last transaction date done by client.
In case of Dormant account the term Dormant/Inactive accounts refers to such accounts where no debit transaction had taken place for a continuous period of 1 Year months.

Categories:

1 Year dormant Accounts: are those trading accounts in which trading had not placed since last since last 1 (Year). In this category, the client code shall be marked disabled in our back office as well as in trading platform, so that no trade can be undertaken/punched in his/her client code. If any such client who is willing to re-initiate trading in its account are required to furnish written request letter of re enablement of its UCC which should be signed by the respective client only & not by POA holder.
Very Old dormant Accounts: are those trading accounts in which trading had not placed since last TWO YEAR. Once the any client code lying inactive since Two years, the client code shall be marked as disabled in our back office as well as in trading platform, so that no trade can be undertaken/punched in his/her client code. If any such client who is willing to re-initiate trading in its account are required to fulfill KYC formalities along with a written request letter of re-enablement of its UCC which should be signed by the respective client only & not by POA holder.

Procedure to be followed:

- A list of inactive clients shall be prepared from the back office software at regular interval and shall be submitted to the concerned department after confirmation with the management. The management will approve a final list of inactive clients.
- A copy of the list is also forwarded to dealers who operate our BOLT or NEAT terminals.
- The concerned department shall mark the client status as “inactive” or “dormant” in various front office software of CTCL and IML and back office accounting and DP software.
- After inactive marking, if any orders are received the dealer shall take reasonable steps to identify the identity of the client and to ensure that the orders are received from the same client. The dealer shall use various techniques like call back, asking personal detail questions, last trade dates, outstanding positions etc to confirm the identity of the caller. They may use any other technique which is reasonable. In case of a doubt the case shall be referred to the management or concerned Sub-Broker or introducer.
- Dormant client/ Block client has to update their KYC details at the time of fresh order, if required.

Annexure

ACCOUNT RE-ACTIVATION FORM

Date: _____

To

Open Futures & Commodities Pvt. Ltd.,
Regd Office: Flat No. 407, 4th Floor,
Palm Spring Plaza, Sector – 54
Golf Course Road, Gurgaon, Haryana - 122001

(To be filed by Client)

Client Code	
Client Name	

I/We hereby request you to re-activate my /our account and treat this form as intimation for re-opening of the account. I/We hereby confirm that all the information provided to you with initial account opening is the same and I/We agree to abide by the exchange rules and notifications issued till date.

Client's Signature

Date.

Policy for Client Code Modification

3. Objective

To frame the guidelines for modification to client codes post trade execution and reporting of such Client Code Modifications and to fulfill compliance in accordance with SEBI requirement or, *(With reference to SEBI circular ref. no. CIR/DNPD/6/2011 dated July 5, 2011, NSE/INVG/2011/18484 and BSE Notice no :20110729-24, Notice date : Friday, July 29, 2011).*

4. Brief about Client Code Modification:

Client Code Modification means modification / change of the client codes after execution of trades. Stock Exchanges provide a facility to modify any client code after the trade has been executed to rectify any error or wrong data entry done by the dealers at the time of punching orders. However, such Client Code modification is subject to certain guidelines as to the time limit within which the client code modification is to be carried out, terminal / system on which such modifications can be done etc. The facility is mainly to provide a system for modification of client codes in case genuine errors in punching / placing the orders. It is to be used as an exception and not a routine. To prevent misuse of the facility Stock Exchanges levy penalty / fine for all non-institutional client code modifications.

5. Scope of the Policy:

This policy covers all the Client Code Modifications carried out / to be carried out in any of the client accounts controlled by HO, subject to the guidelines issued by the SEBI / Stock Exchanges from time to time, in any segment of any exchange for which **Open Futures & Commodities Pvt. Ltd** is a Stock broker.

6. **"Error Trades"** means the trades which will be modified / to be modified / allowed, to be modified subject to guidelines of the SEBI / Stock Exchanges and this policy.

For the purpose of this Policy, only the following types of trades shall be modified / allowed to be modified:

In case of NSE (NOTE: no consistent pattern in such modifications):

1.1. client code/name and modified client code/name are similar to each other but such modifications are not repetitive.

1.2. Family Code (spouse, dependent parents, dependent children and HUF)

In Case of BSE:

J. 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.

K. Trade entered for wrong client due to any miscommunication from the client / authorized representative of the client.

L. Modification within family members
M. Institutional trades modified to broker error/pro account

In Case of MCX

i. 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.

ii. Trade entered for wrong client due to any miscommunication from the client / authorized representative of the client.

5. General Conditions:

6 The facility for Client Code Modification can be used only in case of Error Trade.
7 The Client Code Modification shall be carried out only on the designated system and / or as per the process as may be prescribed by SEBI / Stock Exchange.

6. Place for Client Code Modification:

Any Client Code Modification shall, subject to compliance of this policy, be carried out by RMS at HO of all the Error Trades happened in Capital Market Segment of NSE, BSE and MCX.

7. Penalty

The penalty or fine, if any, levied on **Open Futures Group** for any wrong trade occurred due to any miscommunication from the client / authorized representative of the client shall be borne by the client.

Policy on Outsourcing

KYC documents: Storage & Retrieval

1 Preamble:

Open Futures & Commodities Pvt. Ltd. (in short "OFCPL" or "Company") is a SEBI Registered Intermediary as a **Stock Broker.** Accordingly, it is required that OFCPL shall render at all times high standards of service and exercise due diligence and ensure proper care in its operations.

SEBI being a regulatory authority has mandated to all the intermediaries registered with it to comply with various regulatory requirements and guidelines from time to time. One such **Guideline on Outsourcing of Activities by** Intermediaries has been issued by SEBI vide its Circular no. CIR/MlRSD/24/'2011 dated December 15, 2011.

As per these guidelines, Outsourcing means the use of one or more than one third party ["outsourcer(s)"] — either within or outside the group — by a registered intermediary to perform the activities associated with services which the intermediary offers. In other terms, outsourcing involves transferring responsibility for carrying out an activity of an intermediary (previously carried on internally) to an outsourcer for an agreed charge. The outsourcer provides services to the customer (intermediary) based on a mutually agreed service level, normally defined as per mutual terms and conditions or as per a formal contract.

Many commercial benefits have been ascribed to outsourcing, the most common amongst these being:

Reducing the organization's costs Greater focus on core business by outsourcing non-core functions Access to world-class skills and resources Accordingly, OFCPL announces this Outsourcing policy.

Though Open Futures & Commodites Pvt. Ltd. is currently not outsourcing any business activity.

2 Objective:

In order to guide the Board (means Board of Directors of OFCPL) about the assessment of whether and how the outsourced activity(ies) can be outsourced, this comprehensive policy is being announced and implemented. The objective of this policy is to further specify inter-alia about (i) the scope of policy (ii) criteria to select an outsourcer (iii) nature of activities to be outsourced (iv), various controls to reduce the risks associated with outsourcing and (v) to ensure the high standards of services all the time as well as proper care in OFCPL's operations.

3 Scope:

The policy applies throughout **ORGANIZATION. Open Futures & Commodities Pvt. Ltd.** shall follow various principles for outsourcing as may be prescribed by SEBI in the captioned circular dated 15th December, 2011.

4 Policy **Segments:**

4.1 Choosing *an outsourcer*

OFCPL shall invite bids from various parties to act as the Outsourcer for the Company. While selecting an outsourcer, OFCPL shall inter-alia take into account the following:

Outsourcer's resources and capabilities Its financial soundness and capabilities to perform the work within fixed timelines Compatibility of the practices and systems of an outsourcer Outsourcer's business reputation and past track record Quality of services provided to other customers Location of an outsourcer

4.2 Nature of Activities **outsourced/** *to* **be** *outsourced*

Currently Open Futures & Commodities Pvt. Ltd. is not outsourcing any business activities.

However, the core business activities such as compliance functions, execution of orders and monitoring of trading activities of clients, dematerialization of securities, investment related activities, KYC requirements as per SEBI (KRA) Regulations, 2011 etc. shall not be outsourced.

4.3 Authorities *approving* Activities

The Board of Directors of the Company shall be responsible for approving the activities outsourced / to be outsourced. However, the review of the activities outsourced shall be done by the Management Committee of Board of Directors of OFCPL at regular intervals as it may deem fit in the wake of changing business environment.

4.4 Review ***of Policy and Assessing Outsourcing Risks***

In addition to the regular review and monitoring of outsourcing policy, the Management Committee shall have overall responsibility for ensuring that all the ongoing outsourcing decisions taken by the Company and the activities undertaken by the third party are in consonance with the outsourcing policy.

Further the Management Committee shall be responsible for assessing and evaluating the risks during the review of the outsourcing activities and take necessary action in case if any discrepancy is found during the process. The risks associated with outsourcing can be categorized as operational risk, reputational risk, legal risk, country risk, exit-strategy risk, counter party risk, etc

5. Risk Management Program:

5.1 Evaluation of Third Party

As a part of comprehensive outsourcing risk management program, the Management Committee shall assess the materiality of the outsourced activity based on the following factors:

a) The impact of failure of third party to adequately perform the activity, on the financial, reputational and operational performance of the Company and on the investors / clients;
b) Ability of the Company to cope up with the work, in case of non performance or failure by third party by having suitable back-up arrangements;
c) Regulatory status of third party including its fitness and probity status;
d) Situations involving conflict of interest between the Company and the third party and the measures put in place by the Company to address such potential conflicts, etc.

The result of the risk assessment shall be presented to the Board of Directors for approval prior to signing/ renewing the outsourcing contract. Board of Directors shall decide whether the Company will benefit overall by

outsourcing the function to the outsourcer, taking into account the above factors as presented by the Management Committee. If the risks involved are high and the commercial benefits are marginal (e.g. if the controls necessary to manage the risks are too costly), the function shall not be outsourced.

5.2 Outsourcing to Related Party

In case the Company is desirous of appointing any group entity/ associate of the Company as the third party for outsourcing of activities, it shall take due care and ensure that an arm's length distance has been maintained between the Company and the related third party in terms of infrastructure, manpower, decision-making, record-keeping, etc. for avoidance of potential conflict of interests. Necessary disclosures shall be obtained by the Company from the third party and further the Company shall ensure that the risk management practices adopted by the Company while outsourcing to a related party or an associate would be identical to those followed while outsourcing to an unrelated party.

5.3 Maintenance of Records

The records relating to all activities outsourced shall be preserved centrally

i.e. at the Corporate/ Head office so that the same is readily accessible for review by the Board and/ or Management Committee as and when needed. Management Committee shall ensure that such records are regularly updated and may also form part of the corporate governance review by the management.

5.4 Reviews *by Internal or External Auditors*

Wherever felt necessary, the Board shall mandate regular reviews by internal or external auditors of the outsourcing policies, risk management system and requirements of the regulator. Further, the financial and operational capabilities of the third party in order to assess its ability to continue to meet its outsourcing obligations shall be reviewed as and when deem fit and proper.

6 Accountability of the Company:

1) OFCPL shall be fully liable and accountable for the activities that are being outsourced to the same extent as if the service were provided in-house.
2) Outsourcing arrangements shall not affect the rights of an investor or client against the Company in any manner. The Company shall be liable to the investors for the loss incurred by them due to the failure of the third party and also be responsible for redressal of the grievances received from investors arising out of activities rendered by the third party.

3) The facilities / premises / data that are involved in carrying out the outsourced activity by the third party shall be deemed to be those of the Company and that the Company itself and Regulator or the persons authorized by it shall have the right to access the same at any point of time.
4) Outsourcing arrangements shall not impair the ability of SEBI/SRO or auditors to exercise its regulatory responsibilities such as supervision / inspection of the Company.

7 Due Diligence and Monitoring of the Third Part:

The Company shall all the time exercise due care, skill, and diligence in the selection of the third party and ensure that the third party has the ability and capacity to undertake the provision of the service effectively.

1.2.1 The due diligence undertaken by the Company shall include assessment of:

a. third party's resources and capabilities, including financial soundness, to perform the outsourcing work within the timelines fixed;
b. compatibility of the practices and systems of the third party with the intermediary's requirements and objectives;
C. market feedback of the prospective third party's business reputation and track record of their services rendered in the past;
d. level of concentration of the outsourced arrangements with a single third party; and
e. the environment of the state/ country/ region where the third party is located.

8 Contract and Agreements:

1.2.2 A formal contract between the Company and the outsourcer shall be entered to protect the interest of both the parties. Proper care shall be taken to ensure that the Outsourcing contract:

a) clearly defines what activities are going to be outsourced, including appropriate service and performance levels;
b) provides for mutual rights, obligations and responsibilities of the Company and the outsourcer, including indemnity;
c) provides for the liability of the outsourcer to the Company for unsatisfactory

1.2.3 performance/ other breach of the contract

d) provides for the continuous monitoring and assessment by the Company of the outsourcer so that any necessary corrective measures can be taken up immediately, i.e., the contract shall enable the Company to retain an appropriate level of control over the outsourcing and the right to intervene with appropriate measures to meet legal and regulatory obligations;

e) includes, where necessary, conditions of sub-contracting by the Outsourcer;

has unambiguous confidentiality clauses to ensure protection of proprietary and customer data during the tenure of the contract and also after the expiry of the contract;

g) specifies the responsibilities of the outsourcer with respect to the IT security and contingency plans, insurance cover, business continuity and disaster recovery plans, force majeure clause, etc.;

h) provides for preservation of the documents and data by outsourcer;

i) provides for the mechanisms to resolve disputes arising from implementation of the outsourcing contract;

j) provides for termination of the contract, termination rights, transfer of information and exit strategies;

k) neither prevents nor impedes the Company from meeting its respective regulatory obligations, nor the regulator from exercising its regulatory powers; and

l) provides for the Company and /or the regulator or the persons authorized by it to have the ability to inspect, access all books, records and information relevant to the outsourced activity with the outsourcer.

9 <u>Contingency Plans</u>:

The Company and its outsourcer shall establish and maintain contingency plans, including a plan for disaster recovery and periodic testing of backup facilities. Specific contingency plans shall be separately developed for each outsourcing arrangement, as is done in individual business lines. Further:

a) The Company shall take appropriate steps to assess and address the potential consequence of a business disruption or other problems at the Company's level as well as at the outsourcer's level.

b) It shall consider and co-ordinate the contingency plans at both the levels

c) To ensure business continuity, robust information technology security is a necessity. A breakdown in the IT capacity may impair the ability of the Company to fulfill its obligations to other market participants/ clients/ regulators and could undermine the privacy interests of its customers, harm the Company's reputation, and may ultimately impact on its overall operational risk profile. The Company shall, therefore, seek to ensure that the outsourcer maintains appropriate IT security and robust disaster recovery capabilities.

d) Periodic tests of the critical security procedures and systems and review of the backup facilities shall be undertaken by the Company to confirm the adequacy of the outsourcer's systems.

10 Confidentiality:

The Company shall take appropriate steps to require that the outsourcer protects confidential information of both the Company and its customers from intentional or inadvertent disclosure to unauthorized persons. The Company shall take proper care to:

a) protect its proprietary and confidential customer information and ensure that it is not misused or misappropriated.

b) ensure that the employees of the outsourcer have limited access to the data handled and only on a "need to know" basis and the outsourcer shall have adequate checks and balances to ensure the same.

In cases where the outsourcer is providing similar services to multiple entities, the Company shall ensure that adequate care is taken by the outsourcer to build safeguards for data security and confidentiality.

In instances, where the Outsourcer acts as an outsourcing agent for multiple intermediaries, the Company shall take proper care and ensure that strong safeguards are put in place so that there is no co-mingling of information / documents, records and assets.

11 Disclaimer:

This Outsourcing Policy is prepared by **Open Futures & Commodities Pvt. Ltd. ("OFCPL")** in terms of SEBI's Circular No. CIR/MIRSD/24/2011 dated 15 h December, 2011 for internal circulation only. The use of this Policy or any matter contained herein, in any manner, without the express written permission from OFCPL may lead to legal proceedings against the user at the sole discretion

Reg. Office : Flat No. 407, 4th Floor, Palm Spring Plaza, Sector - 54 Golf Course Road, Gurgaon, Haryana - 122001

Corp. Office : 403, Chiranjeev Tower,43 Nerhru Place,New Delhi – 110019

Company Policies

(Policy shall be reviewed as and when necessary.)

EFFECTIVE DATE(S)

This Policy is effective from April 03, 20011. Last reviewed in Jan, 18th, 2021

Document Approval Dates:

Approved by: Designated Director

Approved Date: 03/11/2016
Review Date: Dec 5th 2011 Reviewer: Compliance Officer
Review Date: June 5th 2012 Reviewer: Compliance Officer
Review Date: Aug 17th 2013 Reviewer: Compliance Officer
Review Date: Jan 17th 2014 Reviewer Compliance Officer
Review Date: Oct. 01st 2015 Reviewer Compliance Officer
Review Date: Feb. 01st 2016 Reviewer Compliance Officer
Review Date: July 11th 2016 Reviewer Compliance Officer
Review Date: Oct. 14th 2016 Reviewer Compliance Officer
Review Date: May23rd 2018 Reviewer Compliance Officer
Review Date: Jan 7th 2020 Reviewer Compliance Officer
Review Date: Jan 18th 2021 Reviewer Compliance Officer