OFFICE MANAGEMENT

NoticeBoard

1. Display of permanent nature Notice Board (viz. painted board) containing required details, at all places where trading terminals are located including registered offices and branch offices of trading Member/Sub-Broker
2. Display of copy of SEBI Registration Certificate

Related to Trading Terminals

1. Trading Terminal to be located at registered offices or Branch Offices or Authorised Person Office
2. Trading Terminal to be operated by Approved Persons only having NISM / NCFM Certification
3. Upload of CTCL Terminal details to the Exchange before activation
4. All information to be correctly uploaded in the prescribed format particularly User Name, location of the terminal and CTCL ID
5. Any change in the uploaded details to be immediately uploaded to the Exchange
6. Due diligence to be exercised while allotting trading terminal and prevent misuse
7. PRO Trading to be done only from trading terminals enabled for PRO trading

Officer

1. Trading Member to Appoint Compliance Officer to monitor the Regulatory requirements and redress Investor's grievances.

Inspection

Trading member to inspect periodically

a. Active Sub-Brokers
b. Active Branches
c. Active Authorised Persons

Branch Management:

1. Make necessary arrangements for uploading of necessary information with Exchanges
2. Make sure to display Notice Board and Name of the company as per the Exchanges
3. Make sure to display SEBI Certificate on the office
4. Make sure to display Investors Do's and Don'ts on the office.

Access Control Policy

1. **SILVER STREAM EQUITIES PRIVATE LIMITED (SSEPL)** implements Department wise Access Control, KYC Department, Accounts Department, Dealing Room, RMS Cabin, Server Room and all the systems are password protected in order to provide authorised, granular and appropriate User access and to ensure appropriate preservation of data Confidentiality, Integrity and Availability in accordance with the Information Security Management Policy.

2. Access Control systems allows the authorised entries only to the above said departments in place to protect the interests of all Users of **SSEPL**

3. This policy applies to all **SSEPL** Networks, IT systems and Authorised Users.

4. The allocation of Privilege Rights shall be restricted and controlled by the IT Department. Technical Teams will safe guard in issuing of privilege rights to entire teams to prevent loss of confidentiality.

5. Access rights will be followed accordingly as per Company Policies and Procedures

6. Every user should attempt to maintain the security of data at its classified level even if technical security mechanisms fail or are absent.

7. Users elected to safe guard the Information or Logs on Digital Media or Storage Devices or Maintaining a Separate Database must only do so where such an action is in accord with the data's classification, and are consequently responsible for ensuring that Data Security, Confidentiality, and Integrity are maintained in accord with the Data Security Policy.

8. Users are obligated to report instances of Non-Compliance to the **SSEPL** Compliance Officer.

9. Access to **SSEPL** IT resources and services will be given through the provision of a Unique Password.

10. No access to any IT resources and services will be provided without prior Authentication

11. Password issuing, strength requirements, changing and control will be managed through formal processes. Password issuing will be managed by IT Helpdesk. Password length, complexity and expiration times will be controlled.

12. Access to Confidential, Restricted and Protected information will be limited to Authorised Persons whose job responsibilities require it, as determined by the data owner or their designated representative, and as stipulated in the Data Security Policy. Requests for access permission to be granted, changed or revoked must be made in writing.

13. Users are expected to become familiar with and abide by **SSEPL** policies, standards and guidelines for appropriate and acceptable usage of the Networks and Systems. All users will have access to expectations, knowledge, and skills related to Information Security.

14. A formal process shall be conducted at regular intervals by **SSEPL** Directors in conjunction with IT Services to review Users' Access Rights. The review shall be logged and IT Services shall Sign Off the review to give Authority for Users continued access rights.