**ANNEXURE F**

**CRITERIA FOR APPLICATION SERVICE PROVIDERS (ASP)**

1. Criteria relating to the back-ground of the ASP. (In case of newly formed company the promoters of the company to fulfil the criteria)

* Suitable organisational structure, promoters and their background. Details of affiliation with other entities like brokers / sub-brokers etc. including beneficial interests held by / in such brokers / sub-brokers etc.
* Track record in project implementation along with good reference sites desirable.
* ISO / CMM certification for IT activity desirable

2. Should have adequate infrastructure in terms of:

* Hardware & software facilities available
* Communication & networking facilities within the organisation
* General office facilities in terms of office space and infrastructure
* Total staff (Minimum no. of 25 technical staff for support)
* Facililites for 24 X 7 Call centre / Help desk

3. System requirements:

* Should have sound platforms for the proposed solution viz whether on NT/UNIX using RDBMS or just pure DOS solution with Dbase type database
* Adequate provisions for system redundancy, fault tolerance and load balancing
* Database redundancy and standby databases (hot standby / cold standby)
* Provisions to monitor system capacity and scalability of system on capacity utilisation
* Contingency planning in case of technical failure and capacity planning (including periodic evaluation of capacity based on historical and anticipated volumes) should be documented and be available for inspection
* Frequency of hardware & software upgrade
* Adequate provisions for back-up systems and data storage
* Alternate means of communication in case of link failure – links to Exchange as well as Internet link failure

4. Security requirements

* Physical security of hardware / systems at hosting location and controls on admission of personnel into location. Audit trail of all entries-exits at location.
* Role based access control of ASP staff to system. Audit trail of all access by ASP staff. Reconfirmation by second user for critical functions (second password).
* Use of authentication technology – user ID and First Level password (private code). Second Level password are advisable
* Automatic expiry of passwords after a reasonable duration and reinitialisation of access on entering fresh passwords
* Encryption of passwords to ensure no unauthorised access to user passwords
* Security, reliability and confidentiality of data related to members and clients. Provisions to ensure that a member / client can see data only pertaining to himself and not other members / clients.
* Records maintained in electronic form should not be susceptible to manipulation
* Logs of all activities / transaction to be maintained with proper audit facilities
* Secured Socket Layer access through Internet – certified by an approved Certifying Authority
* Firewalls between Internet and trading set-up