INTERNAL CONTROL POLICIES

ACCESS TO DEALING ROOM.

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

SOFTWARE SECURITY

LLP is using licensed software for its operations. All computers are protected with Quick Heal Antivirus or Microsoft Security Essential anti-virus. Updation of this software is done online on periodic basis. LLP has also installed Hardware Firewall from Sophos. Configuring the firewall features is the responsibility of the IT staff. This software set up is considered to be sufficient, protecting the IT environment considering the size and operations of the Company.

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

HARDWARE SECURITY

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

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

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

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

DOCUMENTATION POLICY AND INFORMATION STORAGE.

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

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

Documentation is handled by the Compliance Officer of the firm.

PASSWORD POLICY

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

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

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides

at any LLP's facility, has access to the LLP network, or stores any non-public LLP information.

Passwords are used for logging on to System, software in dealing room of LLP.

Password length should be minimum 6 characters, maximum 12 characters & should be alpha-numeric.

All passwords are to be treated as sensitive, Confidential LLP 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 reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation

Change passwords immediately when prompted by ODIN Server.

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

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