Business Continuity Planning / Disaster Recovery Policy

- If the internal live server goes down then the secondary backup manager server which is always on standby mode goes live.
- If anything happens to the lease line then the backup is ISDN Line.
- If anything happens to the primary Airtel internet connection than the Mtnl and Reliance are used as a backup.
- Initial risk assessments are performed to determine current information systems vulnerabilities.
- Initial business impact analysis are performed to document and understand the interdependencies among business processes and determine how the business would be affected by an information systems outage.
- Inventory of information systems assets are being taken such as computer hardware, software, applications, and data.
- Single points of failure are being indentified within the information systems infrastructure.
- Critical applications, systems, and data are being identified.
- Key business functions are being prioritized.
- Offsite facilities for data backup storage and electronic vaulting as well as redundant and reliable standby systems are being setup and maintained.
- It is ensure that the critical applications, systems, and data are distributed among facilities that are reasonably easy to get to but not so close that they could be affected by the same disaster.
- Continuously data backups are being performed, stored weekly backups on offsite, and those backups are tested regularly for data integrity and reliability.

- Training plan for security awareness and disaster recovery education to all the staff is in process.

- We have planned for another backup server at our Delhi branch so if anything happens to our HO premises; the Odin can be broadcasted from our Delhi branch. The backup server will be ready as soon as the IBT goes live.