ELECTRONIC DATA BACKUP POLICY STATEMENT

This policy defines the electronic data backup strategy within Entrepose Delattre Bezons Nigeria Limited (Ent DBN) which is expected to have their data backed up. Servers expected to be backed up include the file server, the mail server, and the web server. This policy applies to all Ent DBN bases and project sites that develop create and/or store critical data in electronic format.

Ent DBN maintains a large number of project data stored exclusively in electronic form. Much of these data are critical to the operation of Ent DBN, and it is clear that we could suffer significant loss should an important set of data be permanently lost.

During the Backup process, electronic data are saved onto magnetic tape or other offline mass storage media for the purpose of retrieving it in case of loss of original data.

The policy is intended to ensure the integrity, availability, and confidentiality of electronically maintained data, including but not limited to confidential, sensitive, or personally identifiable information and that Ent DBN bases are able to resume activities in the event of any incident that causes data loss; hardware failure, inadvertent user error, fire, flood, vandalism, etc..

We maintain multi location data servers. These servers are configured to perform full, incremental, and differential data backup and follow a predefined schedule. Our server ensures that our data is transmitted in a secure and safe environment. It also prevents data snooping during transmission.

All our servers are safeguarded and can only be accessed via a secure authentication process. This prevents unauthorized access to data stored on these servers. In addition to this, all servers are monitored round the clock to ensure that they function seamlessly. It also ensures that sensitive data is not accessible to anyone unauthorised within or outside the organization.

Backups of the file systems are run on a daily basis, usually after the normal working hours. There shall be a separate or set of tapes / Storage device for each backup day.

Daily Backups tapes / Storage device shall be kept for a minimum of one week and used again the following appropriate day of the week.

Every month, a monthly backup tape / Storage device shall be made using the oldest backup tape / Storage device. Monthly backups tapes / Storage devices shall be kept for minimum three months and used again the following appropriate month.

The Network Administrator or his designee shall be responsible for performing regular backups. The backup system does not save files stored on local computer drives nor does it save personal folders. Individual users are solely responsible for their own backups to prevent loss of data.

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

Backup shall be stored in a fireproof safe. Daily backup shall be stored at locations and monthly backup shall be stored in our other facility or corporate office.

The ability to restore data from backups shall be tested at least once in every month.

This Policy is issued with my authority and approval and all concerned are responsible for compliance with its provisions.

Johan MEKKAOUI
Managing Director
May, 2017