Data Protection Policy for Bridges Retreat Centre Franschhoek NPC

The Company commits to continually uphold that the person responsible for instructing the Information Technology contractors to the Company, is the person responsible for the processing of the information.

The Company addressed all security on all personal information. Personal information is at least secure, but not limited to, in the following areas:

1. On end-points;
2. Data in transit;
3. Data stored in cloud;
4. In terms of antivirus, malware, Trojans, worms, phishing employed etc.

All Company officials, employees, vendors and clients are appropriately informed of measures taken to protect personal information and the processing of personal information. Unauthorized persons have no access to personal information and all persons who do have access, have minimum appropriate access to personal information.

Those who hold or process information consent to full surveillance of processing of personal information and consented to personal accountability for such processing. All operators and processors committed to protect personal information and to procure instruction from the responsible party on deemed processing.

The Company procured the commitment of all operators and processors of personal information to employ maximum security and secrecy on all personal information, and to personally assume the responsibility to employ measures to protect personal information on all electronic equipment.

Mobile devices are to be treated like firearms. Devices are always kept on the processor's person. Neither the device nor any information on the device is ever given to third parties who do not hold the written consent of the data subject. Business data will always be kept separate from personal data – i.e., personal information.

Data is encrypted in order to safeguard data against unauthorized exposure to third parties. Data pertains to non-electronic files, end-point data, data in transit and hosted or cloud data. Least number of security codes are kept by least number of employees. The data specialist appointed by the Company will take into account all risk factors and address same to the satisfaction of the POPI Act. Where possible, the number of data storages is maximized.

The Company has done a risk and impact assessment on all cloud computing and is satisfied that its cloud computing adheres to the requirements of the POPI Act.

All non-electronic personal information is kept safe and rules and regulations are applicable to access of filing facilities and office spaces. Risk is reduced to the minimum on all aspects of processing personal information in that information is held behind the maximum practical guarded physical barriers as the environment allows.

All handlers of physical security acknowledged that they are responsible for compliance and undertake to ensure full compliance to the POPI Act. All personal information will always be kept and attended to in a secure manner.

Personal information is only used for the purpose obtained as instructed by the data subject.