Data Protection and Information Sharing Policy

CBOS (PTY) LTD

1. INTRODUCTION

This Data Protection and Information Sharing Policy describes the way that CBOS (Pty) Ltd, (the "Company"), and all of its subsidiaries will meet its legal obligations and requirements concerning confidentiality and information security standards. The requirements within the Policy are primarily based upon the Protection of Personal Information Act, No. 4 of 2013, as it is the key piece of legislation covering security and confidentiality of personal information.

The Company guarantees its commitment to protecting its staff, client's and supplier's privacy and ensuring that their personal information is used appropriately, transparently, securely and in accordance with applicable laws.

2. SCOPE OF THE POLICY

The Policy applies to all Company employees, directors, sub-contractors, agents, and appointees. The provisions of the Policy are applicable to both on and off-site processing of personal information.

3. POLICY STATEMENT

The Company collects and uses Personal Information of the individuals and corporate entities with whom it works in order to operate and carry out its business effectively. The Company regards the lawful and appropriate processing of all Personal Information as crucial to successful service delivery

and essential to maintaining confidence between the Company and those individuals and entities who deal it. The Company therefore fully endorses and adheres to the principles of the Protection of Personal Information Act ("POPI").

4. PROCESSING OF PERSONAL INFORMATION

4.1. The Company will be processing personal information in its possession for the following purposes:

- For the administration and deliverables of contractual agreements.
- Processing orders for products and or services to customers.
- In the course of detecting and prevention of fraud, crime, money laundering and other malpractice.
- Processing of personal information in the event of legal proceedings.
- For the purposes of staff administration.
- Keeping accounting records in accordance with good accounting practices.
- To comply with any legal or regulatory requirements.
- For the purposes of conducting due diligence checks on prospective suppliers and sub-contractors and clients.
- For audit and record keeping purposes.
- For commercial invoicing purposes.
- For executing a legal request from a client in terms of an agreement.
- To collect and store personal information and data provided by clients on centralised servers and software.
- To provide a platform for the storage, organization and interpretation of data and personal information on the client's request.
- Only when consent is obtained from the data subject.

4.2. Types of data subjects and the personal information that will be processed:

- **Customers that are Juristic Persons**: Names of contact persons; name of legal entity; physical and postal address and contact details; financial information; registration number; founding documents; tax related information; authorised signatories; beneficiaries; ultimate beneficial owners; shareholding information; B-BBEE information; any other personal information required by law.
- Contracted Service Providers / Contractors / Sub-contractors / Suppliers: Names of contact persons; name of legal entity; physical and postal address and contact details; financial information; registration number; founding documents; tax related information; authorised signatories; beneficiaries; ultimate beneficial owners; shareholding information; B-BBEE information.
- Employees / Directors / Independent Contractors / Consultants: Gender; marital status; colour, race; age; language; education information; financial information; employment history; ID number; physical and postal address; contact details; opinions; criminal record; well-being.

The above-mentioned personal information will only be processed if the relevant consent is obtained.

5. DISCLOSURE OF PERSONAL INFORMATION TO THIRD PARTIES

The Company may share the Personal Information with its agents, affiliates, and associated companies who may use this information for the purposes envisaged above. The Company may supply the Personal Information to any party to whom the Company may have assigned or transferred any of its rights or obligations under any agreement, and/or to service providers who render the following services, Capturing or organising data, storing data, conducting

due diligence, providing human resources services, for the administration of medical schemes and to perform an obligation under a written agreement.
The Company may also disclose personal information where it has a duty or a right to disclose in terms of applicable legislation, the law, or where it may be deemed necessary to protect the Company's rights. Personal Information may also be disclosed to the Company's clients should it be required under obligation of a concluded agreement or for any vested commercial interest. Personal information may also be transferred to third parties on the instruction of the Company's client. In the event that the company is a 3rd party recipient of personal information the client acknowledges that prior consent was obtained from the data subject.

6. SAFEGUARDING PERSONAL INFORMATION

- It is a requirement of POPI to adequately protect personal information. The Company will continuously review its security controls and processes to ensure that personal information is secure. The following procedures are in place in order to protect personal information.
- The Company's information officer (whose details are available below) is responsible for the compliance with the conditions of the lawful processing of personal information and other provisions of POPI. The information officer is assisted by other information officers in the Company and also assisted by their respective deputies.
- This Policy has been put in place throughout the Company and training on this policy and the POPI Act has taken place throughout the whole Company and its affiliated and subsidiary companies.
- Each new employee will be required to sign an employment contract containing relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of POPI.

- Every employee currently employed within the Company will be required to sign an addendum to their employment contracts containing relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of POPI.
- The Company's archived personal information is stored on site, which is also governed by POPI, access is limited to these areas to authorized personnel.
- All personal information stored on the Company's online systems are subject to access control and security measures.
- The Company's product suppliers, insurers, associated companies, clients and other third-party service providers will be required to sign a service level agreement guaranteeing their commitment to the Protection of Personal Information; this is however an ongoing process that will be evaluated as needed.
- All electronic files or data are backed up by the Company's IT Division which is also responsible for system security that protects third party access and physical threats. The Company IT Division is responsible for Electronic Information Security.
- The Company employs up to date technology to ensure the confidentiality, integrity and availability of the Personal Information under its care, these include: Firewalls, Virus protection software and updated protocols, Logical and physical access control; Secure setup of hardware and software making up the IT infrastructure; Outsourced Service Providers who process Personal Information on behalf of the Company are contracted to implement similar security controls.

7. ACCESS OF PERSONAL INFORMATION

Data subjects have the right to access their personal information as held by the Company. Data Subjects also have the right to request the Company to

update, correct or delete their personal information on reasonable grounds. Once a client objects to the processing of their personal information, the Company may no longer process said personal information, except where it is still permitted under a provision of the POPI or any other applicable law. The Company will take all reasonable steps to confirm its clients' identity before providing details of their personal information or making changes to their personal information.

8. ACCOUNTABILITY

The Company shall ensure that all processing conditions, as set out in POPI, are complied with when determining the purpose and means of processing Personal Information and during the processing itself. The Company shall remain liable for compliance with these conditions, even if it has outsourced it processing activities.

9. PROCESSING LIMITATION:

- The processing of Personal Information is only lawful if, given the purpose of processing, the information is adequate, relevant, and not excessive.
- The Company may only process Personal Information if one of the following grounds of lawful processing exists: The Data Subject consents to the processing; Processing is necessary for the conclusion or performance of a contract with the Data Subject; Processing complies with a legal responsibility imposed on the Company; Processing protects a legitimate interest of the Data Subject; Processing is necessary for pursuance of a legitimate interest of the Company, or a third party to whom the information is supplied;

- Special Personal Information includes: Religious, philosophical, or political beliefs; Race or ethnic origin; Trade union membership; Health or sex life; Biometric information (including blood type, fingerprints, DNA, retinal scanning, voice recognition, photographs); Criminal behaviour; Information concerning a child.
- The Company may only process Special Personal Information under the following circumstances: The Data Subject has consented to such processing; The Special Personal Information was deliberately made public by the Data Subject; Processing is necessary for the establishment of a right or defence in law; Processing is for historical, statistical, or research reasons If processing of race or ethnic origin is in order to comply with affirmative action laws.
- Personal Information must be collected directly from the Data Subject, unless: Personal Information is contained in a public record; Personal Information has been deliberately made public by the Data Subject; Personal Information is collected from another source with the Data Subject's consent; Collection of Personal Information from another source would not prejudice the Data Subject; Collection of Personal Information from another source is necessary to maintain, comply with or exercise any law or legal right; Collection from the Data Subject would prejudice the lawful purpose of collection; Collection from the Data Subject is not reasonably practicable.

10. INFORMATION QUALITY

The Company shall take reasonable steps to ensure that Personal Information is complete, accurate, not misleading and updated. The Company shall periodically review Data Subject records to ensure that the Personal Information is still valid and correct. Employees should as far as reasonably

practicably follow the following guidance when collecting Personal Information:

- Personal Information should be dated when received.
- A record should be kept of where the Personal Information was obtained.
- Changes to information records should be dated.
- Irrelevant or unneeded Personal Information should be deleted or destroyed.
- Personal Information should be stored securely, either on a secure electronic database or in a secure physical filing system.

11. OPENNESS

The Company shall take reasonable steps to ensure that the Data Subject is made aware of what Personal Information is collected, and the source of the information. Similarly, where the supply of Personal Information is voluntary or mandatory, and the Company shall take reasonable steps to ensure the Data Subject is made aware of the consequences of a failure to provide such information or failure to provide correct information. The Company will communicate whether the Personal Information shall be shared with any third party.

12. WRITTEN RECORDS

Personal Information records should be kept in locked cabinets or safes. When in use Personal Information records should not be left unattended in areas where non-staff members may access them. The Company shall implement and maintain a “Clean Desk Policy” where all employees shall be required to clear their desks of all Personal Information when leaving their desks for any length of time and at the end of the day. Personal Information which is no longer required should be disposed of by shredding. Any loss or

theft of, or unauthorised access to, Personal Information must be immediately reported to the Information Officer.

13. ELECTRONIC RECORDS

All electronically held Personal Information must be saved in a secure database or on the Company's quality management system. As far as reasonably practicable, no Personal Information should be saved on individual computers, laptops or hand-held devices. All computers, laptops and hand-held devices should be access protected with a password, fingerprint or retina scan, with the password being of reasonable complexity and changed frequently. The Company shall implement and maintain a "Clean Screen Policy" where all employees shall be required to lock their computers or laptops when leaving their desks for any length of time and to log off at the end of the day. Electronical Personal Information which is no longer required must be deleted from the individual laptop or computer and the relevant database. The employees must ensure that the information has been completely deleted and is not recoverable. Any loss or theft of computers, laptops or other devices which may contain Personal Information must be immediately reported to the Information Officer, who shall notify the IT department, who shall take all necessary steps to remotely delete the information, if possible.

14. DESTRUCTION OF DOCUMENTS

Documents may be destroyed after the termination of the retention period specified herein, or as determined by the Company from time to time. Each department is responsible for attending to the destruction of its documents and electronic records, which must be done on a regular basis. Files must be

checked in order to make sure that they may be destroyed and also to ascertain if there are important original documents in the file. Original documents must be returned to the holder thereof, failing which, they should be retained by the Company pending such return. Deletion of electronic records must be done in consultation with the IT Department, to ensure that deleted information is incapable of being reconstructed and/or recovered.

15. AMENDMENTS TO THIS POLICY

Amendments to, or a review of this Policy, will take place on an ad hoc basis. Employees and Data Subjects are advised to request periodically for the updated policy to keep abreast of any changes.

16. TRANSBORDER INFORMATION FLOW

The Company shall only transfer personal information outside the borders of the Republic of South Africa in the event that:

- The Party receiving the information is subject to similar data protection laws or policies that are applicable in South Africa.
- The data subject and client has agreed to the transfer of information.
- Such transfer is part of the performance of a contract of which the data subject is party.
- The transfer is for the benefit of the data subject, and it is not reasonably practicable to obtain their consent and that such consent would be likely to be given.

17. INFORMATION BREACH

In the event that, or when reasonable grounds exist to believe, that Personal Information has been accessed by an authorised party, the Company's

employees must immediately notify the Company's Information officer of the unauthorised access. The notice to the Information Officer must be as soon as possible in each specific circumstance.

The Information Officer must as soon as possible inform all affected Data Subjects of the unauthorised access and must also inform the Data Regulator of the breach. The notice must contain a description of the possible consequences of the security compromise. A description of the measures that the responsible party intends to take or has taken to address the security compromise. A recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise. If known to the responsible party, the identity of the unauthorised person who may have accessed or acquired the personal information.

18. INFORMATION OFFICERS

Each of the affiliated and subsidiary companies in the Company will appoint its own Information Officer responsible for Personal Information access and requests from data subjects. All Information Officers and Deputies will report directly to the Company Information Officers, and all responsibilities will be delegated from the Company Information Officer to the other Information officers and deputies.

Company Information Officer:	Gerhardus Jacobus Bouwer
Contact number:	084 511 1771
Email:	gerhard.bouwer@cbos.co.za
Designation:	Chief Information Officer