PROTECTION OF PERSONAL INFORMATION POLICY

ROADLAB LABORATORIES (PTY) LTD

REGISTRATION NUMBER: 2011/005423/07

TABLE OF CONTENTS

1. INTERPRETATION 4

2. INTRODUCTION 8

3. VALUES AND PRINCIPLES 9

4. OBJECTIVES 11

5. SCOPE 12

6. EMPLOYEES' DUTIES AND RESPONSIBILITIES IN RESPECT OF POPIA 13

7. CONSENT, JUSTIFICATION AND OBJECTION 14

8. COLLECTION OF PERSONAL INFORMATION DIRECTLY FROM DATA SUBJECT 15

9. COLLECTION FOR SPECIFIC PURPOSE 16

10. RETENTION AND RESTRICTION OF RECORDS 16

11. FURTHER PROCESSING OF PERSONAL INFORMATION TO BE COMPATIBLE WITH THE PURPOSE OF COLLECTION 17

12. CERTAIN TYPES OF PROCESSING SUBJECT TO PRIOR AUTHORISATION FROM THE INFORMATION REGULATOR 19

13. QUALITY OF INFORMATION 19

14. DOCUMENTATION AND RECORDS 20

15. NOTIFICATION TO DATA SUBJECT WHEN COLLECTING PERSONAL INFORMATION 20

16. SECURITY MEASURES ON INTEGRITY AND CONFIDENTIALITY OF PERSONAL INFORMATION 22

17. INFORMATION PROCESSED BY OPERATOR OR PERSON ACTING UNDER AUTHORITY 22

18. SECURITY MEASURES REGARDING INFORMATION PROCESSED BY OPERATOR 23

19. NOTIFICATION OF SECURITY COMPROMISES 23

20. ACCESS TO PERSONAL INFORMATION 24

21. CORRECTION OF PERSONAL INFORMATION 25

22. PROHIBITION ON PROCESSING OF SPECIAL PERSONAL INFORMATION BY THE COMPANY 26

23. GENERAL AUTHORISATION CONCERNING SPECIAL PERSONAL INFORMATION 26

TABLE OF CONTENTS *(continues)*

24. AUTHORISATION CONCERNING DATA SUBJECT'S RELIGIOUS OR PHILOSOPHICAL BELIEFS ……27

25. AUTHORISATION CONCERNING DATA SUBJECT'S RACE OR ETHNIC ORIGIN …….. 28

26. AUTHORISATION CONCERNING DATA SUBJECT'S TRADE UNION MEMBERSHIP …….. 28

27. AUTHORISATION CONCERNING DATA SUBJECT'S POLITICAL PERSUASION ……..... 28

28. AUTHORISATION CONCERNING DATA SUBJECT'S HEALTH OR SEX LIFE ……..… 29

29. AUTHORISATION CONCERNING DATA SUBJECT'S CRIMINAL BEHAVIOUR OR BIOMETRIC INFORMATION …….. 30

30. GENERAL AUTHORISATION CONCERNING PERSONAL INFORMATION OF CHILDREN ……. 31

31. INFORMATION OFFICER ……..... 31

32. DIRECT MARKETING BY MEANS OF UNSOLICITED ELECTRONIC COMMUNICATIONS …….. 32

33. TRANSBORDER INFORMATION FLOWS ……..... 33

34. ERASURE OF DATA AND RETURN OF DATA MEDIA ……..... 34

35. CONFIDENTIALITY IN GENERAL ……... 34

36. TRAINING ……..... 35

37. THE COMPANY'S POWERS GIVEN BY THE COMPANY AND EMPLOYEES' RIGHTS IN RESPECT OF INSTRUCTIONS ……..... 35

1. INTERPRETATION

1.1 In this Policy and for ease of reference, terms used shall bear the same meanings as provided in the clause below, unless a definition to the contrary appears herein.

1.1.1 **"Biometrics"** means a technique of personal identification based on physical, physiological or behavioural characterisation, including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition.

1.1.2 "**Business Operations"** means internal personnel and financial information, vendor names and other vendor information (including vendor characteristics, services and agreements), purchasing and internal cost information, internal services and operational manuals, and the manner and methods of conducting the client's business.

1.1.3 **"Company"** means the ROADLAB LABORATORIES (PTY) LTD with registration number 2011/005423/07

1.1.4 **"Confidential Information"** means–

1.1.4.1 any information or data relating to the Company (even if not marked as being confidential, restricted, secret, proprietary or any similar designation), in whatever format and whether recorded or not (and if recorded, whether recorded in writing, on any electronic medium or otherwise), which by its nature or content is identifiable as, or could reasonably be expected to be, confidential and/or proprietary to the Company;

1.1.4.2 information relating to the Company's existing and future strategic objectives and existing and future business plans and corporate opportunities, trade secrets, technical information, techniques, know-how, operating methods and procedures;

1.1.4.3 details of costs, sources of materials and customer lists (whether actual or potential) and other information relating to the pricing, price lists and purchasing policies of existing and prospective customers and suppliers of the Company;

1.1.4.4 computer data, programs and source codes, whether relating to the client or a third party; and

1.1.4.5 intellectual property of the Company and/or in respect of which it has rights of use or possession.

1.1.5 **"Consent"** means any voluntary, specific and informed expression agreeing to the processing of personal information.

1.1.6 **"Child"** means a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him- or herself.

1.1.7 **"Data"** means any information relating to a Data Subject which was obtained as a result of a legal agreement between the Responsible Party and Data Subject. The information may be held in hardcopy form (e.g. as written notes relating to a person or as part of a filing system, including card index or filing cabinets structured by name, address or other identifier) or in a form capable of being processed electronically.

1.1.8 **"Data Subject"** means the person to whom personal information relates, including a third party or any natural person or legal company whose personal and/or business details were made known to the Responsible Party.

1.1.9 **"Electronic communication''** means any text, voice, sound or image message sent over an electronic communications network and which is stored in the network or on the recipient's terminal equipment until it is collected by the recipient.

1.1.10 **"Filing system''** means any structured set of personal information, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria.

1.1.11 **"Information"** means any confidential information or personal information.

1.1.12 **"Information System"** means the process of, and tools for, storing, managing, using and gathering of data and communications in an organisation.

1.1.13 **"Information Officer"** of, or in relation to, a–

1.1.13.1 public body, means an information officer or deputy information officer as contemplated in terms of section 1 or 17; or

1.1.13.2 private body, means the head of a private body as contemplated in section 1,

of the Promotion of Access to Information Act 2 of 2000 (PAIA).

1.1.14 **"Information Regulator"** means the Information Regulator established in terms of section 39 of POPIA.

1.1.15 **"Operator"** means a person who processes personal information for a Responsible Party in terms of a contract or mandate, without coming under the direct authority of that party.

1.1.16 **"Personal information** means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to–

1.1.16.1 information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, wellbeing, disability, religion, conscience, belief, culture, language and birth of the person;

1.1.16.2 information relating to the education or the medical, financial, criminal or employment history of the person;

1.1.16.3 any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person;

1.1.16.4 the biometric information of the person;

1.1.16.5 the personal opinions, views or preferences of the person;

1.1.16.6 correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;

1.1.16.7 the views or opinions of another individual about the person; and

1.1.16.8 the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

1.1.17 **"Personal Requester"** means a requester seeking access to a record containing personal information about the requester himself/herself.

1.1.18 **"PAIA"** means the Promotion of Access to Information Act (Act No 2 of 2000).

1.1.19 **"Processing"** means any operation or activity, or any set of operations whether or not by automatic means, including–

1.1.19.1 the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;

1.1.19.2 dissemination by means of transmission, distribution or made available in any other form; or

1.1.19.3 merging, linking, as well as restriction, degradation, erasure or destruction of information.

1.1.20 **"POPI"** or **"POPIA"** means the Protection of Personal Information Act (Act No. 4 of 2013).

1.1.21 **"Record"** means any recorded information–

1.1.21.1 regardless of form or medium, including any–

1.1.21.1.1 writing on any material;

1.1.21.1.2 information produced, recorded or stored by means of any tape recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored;

1.1.21.1.3 label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;

1.1.21.1.4 book, map, plan, graph or drawing;

1.1.21.1.5 photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced;

1.1.21.2 in the possession or under the control of a responsible party;

1.1.21.3 whether or not it was created by a responsible party; and

1.1.21.4 regardless of when it came into existence.

1.1.22 **"Request"** means a request for access to a record or information of the Company or a Data Subject.

1.1.23 **"Responsible party"** means a public or private body or any other person which or who, alone or in conjunction with others, determines the purpose of and means for processing personal information.

1.1.24 **"Third Party",** in relation to a request for access, means any person, excluding a Data Subject or a personal requester.

1.1.25 **"Special Personal Information"** means personal information as referred to in section 26 of POPIA.

1.1.26 **"this Policy"** or **"the Policy"** means this Protection of Personal Information Policy.

1.1.27 **"the Responsible Party"** means the Company.

1.1.28 **"unique identifier"** means any identifier that is assigned to a Data Subject and is used by a Responsible Party for the purposes of the operations of that Responsible Party and that uniquely identifies that Data Subject in relation to that Responsible Party.

2. INTRODUCTION

2.1 In terms of the Protection of Personal Information Act ("POPI" or "POPIA") 4 of 2013, Roadlab Laboratories (Pty) Ltd (**"the Company"**) is the Responsible Party in respect of the personal information held of other persons such as employees, clients and customers, referred to in POPIA and this Policy as (**"Data Subjects**").

2.2 Whenever the Company, through its employees, representatives, agents or providers of goods and services, processes personal information, data or confidential information of the Company itself or personal information of Data Subjects, the rights of the Company and the Data Subjects are protected by POPIA. The right of Data Subjects to have their personal information protected must be balanced with the rights of certain persons (third parties) who may legitimately seek access to such information. The rights of persons to request information are dealt with in a Manual compiled in terms of the Promotion of Access to Information Act 2 of 2000 (PAIA), which Manual is readily available on the Company's premises, its website or from the Company's Information Officer(s).

2.3 Employees who are granted the privilege of access to personal information and data in the performance of their duties must adhere to strict guidelines regarding the appropriate use of this resource. Employees as users who violate the provisions of legislation and this Policy will be subjected to disciplinary action in terms of the Company's disciplinary codes and procedures. Access to data shall not be used for any illegal or unlawful purposes, i.e. abuse involving criminal offences such as fraud and intimidation. Users must be aware that access to data is strictly limited to activities in direct relation to official business, their duties, job description and the purpose for which it was provided.

2.4 This Policy provides the procedures for the use of any personal information data and records within the Company and will ensure that all policies remain current and relevant. It will, therefore, be necessary from time to time to modify and amend some sections of the policies and procedures, or to add new procedures.

3 VALUES AND PRINCIPLES

3.1 The Company is committed to safeguarding the confidentiality, integrity and availability of all physical and electronic data and personal information of the Company to ensure that regulatory, operational and contractual requirements are met.

3.2 The Company shall ensure that information is accessible only to those authorised to have access, while safeguarding the accuracy and completeness of information when processing and archiving data and personal information.

3.3 In respect of the processing of personal information of Data Subjects, the Company recognises the rights of Data Subjects which can be summarised in terms of POPIA as follows:

3.3.1 **Rights of Data Subjects**

3.3.1.1 A Data Subject has the right to have his/her or its personal information processed in accordance with the conditions for the lawful processing of personal information, including the right–

3.3.1.1.1 to be notified that –

3.3.1.1.1.1 personal information about him/her or it is being collected as provided for in terms of section 18 of POPIA; or

3.3.1.1.1.2 his/her or its personal information has been accessed or acquired by an unauthorised person as provided for in terms of section 22 of POPIA;

3.3.1.1.2 to establish whether a Responsible Party holds personal information of that Data Subject and to request access to his/her or its personal information as provided for in terms of section 23 of POPIA;

3.3.1.1.3 to request, where necessary, the correction, destruction or deletion of his/her or its personal information as provided for in terms of section 24 of POPIA;

3.3.1.1.4 to object, on reasonable grounds relating to his/her or its particular situation, to the processing of his/her or its personal information as provided for in terms of section 11(3)(a) of POPIA;

3.3.1.1.5 to object to the processing of his/her or its personal information;

3.3.1.1.5.1 at any time for purposes of direct marketing in terms of section 11(3)(b) of POPIA; or

3.3.1.1.5.2 in terms of section 69(3)(c) of POPIA;

3.3.1.1.6 not to have his/her or its personal information processed for purposes of direct marketing by means of unsolicited electronic communications except as referred to in section 69 (1) of POPIA;

3.3.1.1.7 not to be subject, under certain circumstances, to a decision which is based solely on the automated processing of his/her or its personal information intended to provide a profile of such person as provided for in terms of section 71 of POPIA;

3.3.1.1.8 to submit a complaint to the Regulator regarding the alleged interference with the protection of the personal information of any Data Subject or to submit a complaint to the Information Regulator in respect of a determination of an adjudicator as provided for in terms of section 74 of POPIA; and

3.3.1.1.9 to institute civil proceedings regarding the alleged interference with the protection of his/her or its personal information as provided for in section 99 of POPIA.

3.3.2 **Exclusions**

3.3.2.1 The provisions of POPIA do not apply to the processing of personal information–

3.3.2.1.1 in the course of a purely personal or household activity;

3.3.2.1.2 that has been de-identified to the extent that it cannot be re-identified again;

3.3.2.1.3 by or on behalf of a public body–

3.3.2.1.3.1 which involves national security, including activities that are aimed at assisting in the identification of the financing of terrorist and related activities, defence or public safety; or

3.3.2.1.3.2 the purpose of which is the prevention and detection, including assistance in the identification of the proceeds of unlawful activities and combating of money laundering activities, investigation or proof of offences, the prosecution of offenders or the execution of sentences or security measures to the extent that adequate safeguards have been established in legislation for the protection of such personal information;

3.3.2.1.4 by the Cabinet and its committees or the Executive Council of a province; or

3.3.2.1.5 relating to the judicial functions of a court referred to in section 166 of the Constitution of South Africa.

1.1.3 Exclusion for journalistic, literary or artistic purposes

3.3.3.1 POPIA does not apply to the processing of personal information solely for the purpose of journalistic, literary or artistic expression to the extent that such an exclusion is necessary to reconcile, as a matter of public interest, the right to privacy with the right to freedom of expression.

1.1.3.2 Where a Responsible Party who processes personal information exclusively for journalistic purposes is, by virtue of office, employment or profession, subject to a code of ethics that provides adequate safeguards for the protection of personal information, such code will apply to the processing concerned to the exclusion of POPIA, and any alleged interference with the protection of the personal information of a Data Subject that may arise as a result of such processing must be adjudicated as provided for in terms of that code.

3.3.3.3 In the event of a dispute as to whether or not adequate safeguards have been provided for in a code as required in terms of paragraph 3.3.3.2 above, consideration may be given to–

3.3.3.3.1 the special importance of the public interest in freedom of expression;

3.3.3.3.2 domestic and international standards balancing the–

3.3.3.3.2.1 public interest in allowing for the free flow of information to the public through the media in recognition of the right of the public to be informed;

3.3.3.3.2.2 public interest in safeguarding the protection of personal information of Data Subjects;

3.3.3.3.2.3 the need to secure the integrity of personal information;

3.3.3.3.2.4 domestic and international standards of professional integrity for journalists; and

3.3.3.3.2.5 the nature and ambit of self-regulatory forms of supervision provided by the profession.

4 OBJECTIVES

4.1 The purpose of this Policy is to establish guidelines and responsibilities for the use of personal information and data in the Company. The Policy includes the basic protocols for regulating the use of the Company's internet facilities, as well as general controls and associated services, to ensure business continuity, minimise business damage and maximise return on business opportunities with a view to protecting the reliability and completeness of all personal information.

4.2 This policy provides guidelines for the following:

4.2.1 Compliance with requirements for confidentiality, integrity and availability of personal information of the Company's employees, clients, suppliers, customers and other stakeholders;

4.2.2 Establishing controls for protecting the Company's own information and information systems against theft, abuse and other forms of harm and loss;

4.2.3 Motivating administrators and employees to meet their responsibilities in terms of ownership of and knowledge about personal information security in order to minimise the risk of security incidents;

4.2.4 Ensuring that the Company is capable of continuing operations even in the event of major security incidents;

4.2.5 General communication practices, social media management and confidentiality of information;

4.2.6 Managing the risk of usage and guiding users as to what is acceptable;

4.2.7 The use of Company-owned or sponsored personal computers, laptops, phones, fax machines, notebooks, printers, electronic devices, related hardware and any Company software;

4.2.8 Access to and disclosure of electronic mail messages sent or received by employees, and storage and printing of confidential and personal information;

4.2.9 To provide for procedures and measures to fulfil the conditions of the lawful processing of personal information in terms of POPIA, which conditions are as follows:

4.2.9.1 'Accountability', as referred to in section 8 of POPIA;

4.2.9.2 'Processing limitation', as referred to in sections 9 to 12 of POPIA;

4.2.9.3 'Purpose specification', as referred to in sections 13 and 14 of POPIA;

4.2.9.4 'Further processing limitation' as referred to in section 15 of POPIA;

4.2.9.5 'Information quality', as referred to in section 16 of POPIA;

4.2.9.6 'Openness', as referred to in sections 17 and 18 of POPIA;

4.2.9.7 'Security safeguards', as referred to in sections 19 to 22 of POPIA; and

4.2.9.8 'Data Subject participation', as referred to in sections 23 to 25 of POPIA.

5 SCOPE

5.1 This Policy applies to all employees of the Company (temporary and permanent) as well as independent contractors who work on the premises of the Company or who have access to the personal information and data of the Company.

5.2 All employees are required to fully understand and comply with the Policy as set out in this document.

5.3 The Company reserves the right to monitor user activities, including phone and internet records, for compliance with information security principles.

5.4 The scope, type and purpose of the collection, processing and/or use of personal information data by employees for the Company are specified in this Policy.

5.5 Every other transfer to a third party requires the prior consent of the Company, which must be given when the special requirements of the applicable provisions of POPIA are met.

5.6 Any reference to **"the Company"** shall also include employees and other persons acting on behalf of the Company.

6 EMPLOYEES' DUTIES AND RESPONSIBILITIES IN RESPECT OF POPIA

6.1 Employees' observation of the provisions of the applicable provisions of POPIA is important to secure the lawful processing of personal information and entails the following duties and responsibilities:

6.1.1 Observation of personal information data confidentiality pursuant to the respectively applicable provisions of POPIA. All persons and employees who have access to personal information data of the Company by virtue of their mandates are obliged to maintain confidentiality of the personal information and data of the Company and must be instructed in the special data protection duties arising from this mandate and the existing instruction and purpose commitment.

6.1.2 The implementation and observation of all technical and organisational measures necessary for this mandate in compliance with the respectively applicable provisions of POPIA.

6.1.3 Immediate notification of the Company with regard to the control procedures and measures of the supervisory authority pursuant to the respectively applicable provisions of POPIA. This also applies should a competent authority investigate employees' conduct in accordance with the respectively applicable provisions of POPIA.

6.1.4 Job control by means of regular checks by employees with regard to the execution or fulfilment of their mandates, in particular the observation and, where applicable, the necessary adaptation of provisions and measures for the performance of their mandates, duties and responsibilities.

6.1.5 Verifiability of the technical and organisational measures implemented by the Company. In this respect employees are required to co-operate with any verifying process. The Company may request, at its own cost, specific attestations, reports or report excerpts of independent bodies (e.g. auditors, audits, data protection officer, Information Technology (IT) security departments, data protection auditor, quality auditor) or appropriate certification by an IT security or data protection audit.

6.1.6 Overall the measures to be implemented relate to organisational control, physical access control, system access control, data access control, transmission control, job control, availability control and separation requirement, and provide guidelines and rules with regard to the type of data exchange / data provision, / the type / circumstances of processing / data storage and the type / circumstances of output / data transmission, especially those relating to personal information data.

6.1.7 The technical and organisational measures are subject to continuous technical progress and further development. In this respect employees are permitted to implement alternative and adequate and appropriate interim measures which may not fall short of the safety level of the specified measures, and which are not inconsistent with this Policy and data protection measures implemented by the Company. All significant and material changes must be documented by employees. On request, employees are obliged to provide the Company with the information stipulated in respect of the applicable provisions of POPIA which they as employees are required to observe.

7 CONSENT, JUSTIFICATION AND OBJECTION

7.1 In terms of POPIA, personal information may only be processed by the Company and persons acting on behalf of the Company if–

7.1.1 the Data Subject or a competent person (as guardian) where the Data Subject is a child, consents to the processing;

7.1.2 processing is necessary to carry out actions for the conclusion or performance of a contract or arrangement for the delivery of goods and services to which the Data Subject is a party;

7.1.3 processing complies with an obligation imposed by law on the Company;

7.1.4 processing protects a legitimate interest of the Data Subject;

7.1.5 processing is necessary for the proper performance of a public law duty by a public body; or

7.1.6 processing is necessary for pursuing the legitimate interests of the Company as Responsible Party or of a third party to whom the information is supplied.

7.2 In terms of section 11(2)(a) of POPIA, the Company bears the burden of proof for the Data Subject's or competent person's (in the event of a child) consent, as referred to in paragraphs 7.1.1 – 7.1.6 above.

7.3 The Data Subject or competent person may withdraw his/her or its consent, as referred to in paragraph 7.1.1 above, at any time: Provided that the lawfulness of the processing of personal

information **before** such withdrawal or the processing of personal information in terms of paragraphs 7.1.2 – 7.1.6 above, will not be affected.

7.4 A Data Subject may object, at any time, to the processing of personal information–

7.4.1 in terms of paragraphs 7.1.4 – 7.1.6 above, in the prescribed manner, on reasonable grounds relating to his/her or its particular situation, unless legislation provides for such processing; or

7.4.2 for purposes of direct marketing other than direct marketing by means of unsolicited electronic communications as referred to in section 69 of POPIA.

7.5 If a Data Subject has objected to the processing of personal information in terms of paragraph 7.4 above, the Company shall no longer process such personal information.

8. COLLECTION OF PERSONAL INFORMATION DIRECTLY FROM DATA SUBJECT

8.1 The Company must collect personal information directly from the Data Subject, except as otherwise provided for in paragraph 8.2 below.

8.2 It is not necessary to comply with paragraph 8.1 if–

8.2.1 the information is contained in or derived from a public record or has deliberately been made public by the Data Subject;

8.2.2 the Data Subject or a competent person where the Data Subject is a child has consented to the collection of the information from another source;

8.2.3 collection of the information from another source would not prejudice a legitimate interest of the Data Subject;

8.2.4 collection of the information from another source is necessary–

8.2.4.1 to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences;

8.2.4.2 to comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue, as defined in section 1 of the South African Revenue Service Act, 1997 (Act No. 34 of 1997);

8.2.4.3 for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated;

8.2.4.4 in the interests of national security; or

8.2.4.5 to maintain the legitimate interests of the Company as Responsible Party or of a third party to whom the information is supplied;

8.2.5 compliance would prejudice a lawful purpose of the collection; or

8.2.6 compliance is not reasonably practicable in the circumstances of the particular case.

9. COLLECTION FOR SPECIFIC PURPOSE

9.1 The Company shall collect personal information for a specific, explicitly defined and lawful purpose related to a function or activity of the Company as Responsible Party.

9.2 The Company shall at all times, in accordance with section 18(1) of POPIA, ensure that Data Subjects are aware of the purpose of the collection of their information unless the provisions of section 18(4) of POPIA are applicable.

10. RETENTION AND RESTRICTION OF RECORDS

10.1 Subject to paragraphs 10.2 and 10.3 below, records of personal information shall not be retained by the Company any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed, unless–

10.1.1 retention of the record is required or authorised by law;

10.1.2 the Company as Responsible Party reasonably requires the record for lawful purposes related to its functions or activities;

10.1.3 retention of the record is required by a contract or arrangement between the Company and the parties thereto; or

10.1.4 the Data Subject or a competent person where the Data Subject is a child has consented to the retention of the record.

10.2 Records of personal information may be retained for periods in excess of those contemplated in paragraph 10.1 for historical, statistical or research purposes if the Company has established appropriate safeguards against the records being used for any other purposes.

10.3 If the Company has used a record of personal information of a Data Subject to make a decision about the Data Subject, the Company shall –

10.3.1 retain the record for such period as may be required or prescribed by law or a code of conduct issued by the Information Regulator; or

10.3.2 if no law or code of conduct prescribes a retention period, retain the record for a period which will afford the Data Subject a reasonable opportunity, taking all considerations relating to the use of the personal information into account, to request access to the record.

10.4 The Company must destroy or delete a record of personal information or de-identify it as soon as reasonably practicable after the Company is no longer authorised to retain the record in terms of paragraphs 10.1 and 10.2 above.

10.5 The destruction or deletion of a record of personal information in terms of paragraph 10.4 above, must be done in a manner that prevents its reconstruction in an intelligible form.

10.6 The Company must restrict processing of personal information if–

10.6.1 its accuracy is contested by the Data Subject, for a period enabling the Company to verify the accuracy of the information;

10.6.2 the Company no longer needs the personal information for achieving the purpose for which the information was collected or subsequently processed, but it has to be maintained for purposes of proof;

10.6.3 the processing is unlawful and the Data Subject opposes its destruction or deletion and requests the restriction of its use instead; or

10.6.4 the Data Subject requests that the personal data be transmitted into another automated processing system.

10.7 Personal information referred to in paragraph 10.6 above may, with the exception of storage, only be processed for purposes of proof, or with the Data Subject's consent, or with the consent of a competent person in respect of a child, or for the protection of the rights of another natural or legal person, or if such processing is in the public interest.

10.8 Where processing of personal information is restricted pursuant to paragraph 10.6 above, the Company must inform the Data Subject before lifting the restriction on processing.

11. FURTHER PROCESSING OF PERSONAL INFORMATION TO BE COMPATIBLE WITH THE PURPOSE OF COLLECTION

11.1 Further processing of personal information by the Company must be in accordance or compatible with the purpose for which it was originally collected in terms of paragraph 9 above.

11.2 To assess whether further processing is compatible with the purpose of collection, the Company must take account of–

11.2.1 the relationship between the purpose of the intended further processing and the purpose for which the information had been collected initially;

11.2.2 the nature of the information concerned;

11.2.3 the consequences and prejudice of the intended further processing for the Data Subject;

11.2.4 the manner in which the information has been collected; and

11.2.5 any contractual rights and obligations between the Company and the Data Subject as to such contract parties.

11.3 Section 15 of POPIA does not consider the further processing of personal information to be incompatible with the purpose of collection if –

11.3.1 the Data Subject or a competent person where the Data Subject is a child has consented to the further processing of the information;

11.3.2 the information is available in or derived from a public record or has deliberately been made public by the Data Subject;

11.3.3 further processing is necessary–

11.3.3.1 to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences;

11.3.3.2 to comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Service At, 1997 (Act No. 34 of 1997);

11.3.3.3 for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated; or

11.3.3.4 in the interests of national security;

11.3.4 the further processing of the information is necessary to prevent or mitigate a serious and imminent threat to–

11.3.4.1 public health or public safety; or

11.3.4.2 the life or health of the Data Subject or another individual;

11.3.5 the information is used for historical, statistical or research purposes and the Company is able to ensure that the further processing is carried out solely for such purposes and will not be published in an identifiable form; or

11.3.6 the further processing of the information is in accordance with an exemption granted by the Information Regulator under section 37 of POPIA.

12. CERTAIN PROCESSING SUBJECT TO PRIOR AUTHORISATION FROM THE INFORMATION REGULATOR

12.1 The Company shall seek authorisation from the Information Regulator, in terms of section 57 of POPIA, prior to any processing if the Company plans to–

12.2 process any **"unique identifiers"** as per paragraph 1.1.28 above, of Data Subjects–

12.2.1. for a purpose other than the one for which the identifier was specifically intended at collection; and

12.2.2 with the aim of linking the information together with information processed by other Responsible Parties;

12.3 process information on criminal behaviour or on unlawful or objectionable conduct on behalf of third parties;

12.4 process information for the purposes of credit reporting; or

12.5 transfer of special personal information, as referred to in section 26 of POPIA, or the personal information of children as referred to in section 34 of POPIA, to a third party in a foreign country that does not provide an adequate level of protection for the processing of personal information as referred to in section 72 of POPIA.

12.6 This paragraph 12 shall not be applicable if a code of conduct has been issued by the Information Regulator and has come into force in terms of Chapter 7 of POPIA in a specific sector or sectors of society.

12.7 The Company shall obtain prior authorisation, as referred to in paragraph 12.1 above, only once and not each time that personal information is received or processed, except where the processing departs from that which has been authorised in accordance with the provisions of paragraph 12.1 above.

13. QUALITY OF INFORMATION

13.1 The Company must take reasonably practicable steps to ensure that the personal information is complete, accurate, not misleading and updated where necessary.

13.2 In taking the steps referred to in paragraph 13.1 above, the Company shall have regard to the purpose for which personal information is collected or further processed.

14. DOCUMENTATION AND RECORDS

14.1 The Company shall maintain the documentation and records of all processing operations under its responsibility as referred to in section 51 of the Promotion of Access to Information Act 2 of 2000 (PAIA).

14.2 For this purpose, the Company has compiled a Manual in terms of PAIA which is available on the Company's business premisses and from the Company's Information Officer.

15. NOTIFICATION TO DATA SUBJECT WHEN COLLECTING PERSONAL INFORMATION

15.1 If personal information is collected, the Company shall take reasonably practicable steps to ensure that the Data Subject is aware of–

15.1.1 the information being collected and, where the information is not collected from the Data Subject, the source from which it is collected;

15.1.2 the name and address of the Company as Responsible Party;

15.1.3 the purpose for which the information is being collected;

15.1.4 whether or not the supply of the information by that Data Subject is voluntary or mandatory;

15.1.5 the consequences of failure to provide the information;

15.1.6 any particular law authorising or requiring the collection of the information;

15.1.7 the fact that, where applicable, the Company intends to transfer the information to a third country or international organisation, and of the level of protection afforded to the information by that third country or international organisation;

15.1.8 the fact that any further information shall be provided by the Company to the Data Subject, such as–

15.1.8.1 the recipient or category of recipients of the information;

15.1.8.2 the nature or category of the information;

15.1.8.3 the right of access to and the right to rectify the information collected;

15.1.8.4 the right to object to the processing of personal information as referred to in section 11(3) of POPIA; and

15.1.8.5 the right of the Data Subject to lodge a complaint with the Information Regulator and be advised of the contact details of the Information Regulator, having regard to the specific circumstances in which the information is or is not to be processed, to enable processing in respect of the Data Subject to be reasonable.

15.2 The steps referred to in paragraph 15.1 above shall be taken by the Company–

15.2.1 if the personal information is collected directly from the Data Subject, before the information is collected, unless the Data Subject is already aware of the information referred to in that subsection; or

15.2.2 in any other case, before the information is collected or as soon as reasonably practicable after it has been collected.

15.3 If the Company has previously taken the steps referred to in paragraph 15.1 above, it would comply with paragraph 15.1 above in relation to the subsequent collection from the Data Subject of the same information or information of the same kind if the purpose of collection of the information remains the same.

15.4 The Company is not required in terms of section 18(4) of POPIA to comply with paragraph 15.1 above if–

15.4.1 the Data Subject or a competent person where the Data Subject is a child has provided consent for the non-compliance;

15.4.2 non-compliance would not prejudice the legitimate interests of the Data Subject as set out in terms of POPIA;

15.4.3 non-compliance is necessary–

15.4.3.1 to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences;

15.4.3.2 to comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Service Act, 1997 (Act No. 34 of 1997);

15.4.3.3 for the conduct of proceedings in any court or tribunal that have been commenced or are reasonably contemplated; or

15.4.3.4 in the interests of national security;

15.4.4 compliance would prejudice a lawful purpose of the collection;

15.4.5 compliance is not reasonably practicable in the circumstances of the particular case; or

15.4.6 the information will–

15.4.6.1 not be used in a form in which the Data Subject may be identified; or

15.4.6.2 be used for historical, statistical or research purposes.

16. SECURITY MEASURES ON INTEGRITY AND CONFIDENTIALITY OF PERSONAL INFORMATION

16.1 The Company shall take responsibility to secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent–

16.1.1 loss of, damage to or unauthorised destruction of personal information; and

16.1.2 unlawful access to or processing of personal information.

16.2 In order to give effect to paragraph 16.1 above, the Company has taken reasonable measures to–

16.2.1 identify all reasonably foreseeable internal and external risks to personal information it its possession or under its control;

16.2.2 establish and maintain appropriate safeguards against the risks identified;

16.2.3 regularly verify that the safeguards are effectively implemented; and

16.2.4 ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

16.3 The Company is compelled in terms of section 19(3) of POPIA to have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations.

17. INFORMATION PROCESSED BY OPERATOR OR PERSON ACTING UNDER AUTHORITY

17.1 An Operator, such as a supplier of goods and services to the Company, or anyone processing personal information on behalf of the Company, must–

17.1.1 process such information only with the knowledge or authorisation of the Company; and

17.1.2 treat personal information which comes to their knowledge as confidential and may not disclose it, unless required by law or in the course of the proper performance of their contractual duties or mandate.

18. SECURITY MEASURES REGARDING INFORMATION PROCESSED BY OPERATOR

18.1 The Company has, in terms of a written contract between the Company and all its Operators, ensured that the Operators which process personal information for the Company establish and maintain the security measures referred to in section 19 of POPIA.

18.2 All Operators are compelled to notify the Company immediately where there are reasonable grounds to believe that the personal information of a Data Subject which they process on behalf of the Company has been accessed or acquired by any unauthorised person.

19. NOTIFICATION OF SECURITY COMPROMISES

19.1 Where there are reasonable grounds to believe that the personal information of a Data Subject has been accessed or acquired by any unauthorised person, the Company shall notify–

19.1.1 the Information Regulator; and

19.1.2 the Data Subject, unless the identity of such Data Subject cannot be established, and the circumstances provided for in terms of paragraph 19.3 below, are present.

19.2 The notification referred to in paragraph 18.1 above must be issued as soon as reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the Company's information system.

19.3 The Company shall only delay notification of the Data Subject if a public body responsible for the prevention, detection or investigation of offences or the Information Regulator determines that notification will impede a criminal investigation by the public body concerned.

19.4 The notification to a Data Subject by the Company referred to in paragraph 19.1 above shall be in writing and communicated to the Data Subject in at least one of the following ways:

19.4.1 mailed to the Data Subject's last known physical or postal address;

19.4.2 sent by e-mail to the Data Subject's last known e-mail address;

19.4.3 placed in a prominent position on the website of the Company;

19.4.4 published in the news media; or

19.4.5 as may be directed by the Information Regulator.

19.5 The notification referred to in paragraph 19.1 above shall provide sufficient information to allow the Data Subject to take protective measures against the potential consequences of the compromise, including–

19.5.1 a description of the possible consequences of the security compromise;

19.5.2 a description of the measures that the Company intends to take or has taken to address the security compromise;

19.5.3 a recommendation with regard to the measures to be taken by the Data Subject to mitigate the possible adverse effects of the security compromise; and

19.5.4 if known to the Company, the identity of the unauthorised person who may have accessed or acquired the personal information.

19.6 The Company shall publicise, in any manner specified by the Information Regulator, the fact of any compromise to the integrity or confidentiality of personal information, if the Information Regulator has reasonable grounds to believe that such publicity would protect a Data Subject who may be affected by the compromise.

20. ACCESS TO PERSONAL INFORMATION

20.1 A Data Subject, having provided adequate proof of identity, has the right to–

20.1.1 request the Company to confirm, free of charge, whether or not the Company holds personal information about the Data Subject; and

20.1.2 request from the Company the record or a description of the personal information about the Data Subject held by the Company, including information about the identity of all third parties, or categories of third parties, who have, or have had, access to the information–

20.1.2.1 within a reasonable time;

20.1.2.2 at a prescribed fee, if any;

20.1.2.3 in a reasonable manner and format; and

20.1.2.4 in a form that is generally understandable.

20.2 If, in response to a request in terms of paragraph 20.1 above, personal information is communicated to a Data Subject, the Data Subject must be advised of the right in terms of section 24 of POPIA to request the correction of information.

20.3 If a Data Subject is required by the Company to pay a fee for services provided to the Data Subject in terms of paragraph 20.1.2 above to enable the Company to respond to a request, the Company–

20.3.1 must give the applicant a written estimate of the fee before providing the services; and

20.3.2 may require the applicant to pay a deposit for all or part of the fee.

20.4 The Company is obliged to refuse, as the case may be, to disclose any information requested in terms of paragraph 20.1 above to which the grounds for refusal of access to records set out in the applicable sections of Chapter 4 of Part 2 and Chapter 4 of Part 3 of the Promotion of Access to Information Act (PAIA) apply. The provisions of sections 30 and 61 of PAIA are applicable in respect of access to health or other records.

20.5 If a request for access to personal information is made to the Company and part of that information may or must be refused in terms of paragraph 20.4 above, every other part must be disclosed.

20.6 All requests for personal information from third parties will be dealt with in terms of the Manual compiled by the Company in terms of section 51 of PAIA.

21. CORRECTION OF PERSONAL INFORMATION

21.1 A Data Subject may, in the prescribed manner, request the Company to–

21.1.1 correct or delete personal information about the Data Subject in its possession or under its control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully; or

21.1.2 destroy or delete a record of personal information about the Data Subject which the Company is no longer authorised to retain in terms of section 14 of POPIA.

21.2 On receipt of a request in terms of paragraph 21.1 above, the Company shall, as soon as reasonably practicable–

21.2.1 correct the information;

21.2.2 destroy or delete the information;

21.2.3 provide the Data Subject, to his or her satisfaction, with credible evidence in support of the information; or

21.2.4 where agreement cannot be reached between the Company and the Data Subject, and if the Data Subject so requests, take such steps as are reasonable in the circumstances, to attach to the information in such a manner that it will always be read with the information, an indication that a correction of the information had been requested but has not been made.

21.3 If the Company has taken steps under paragraph 21.2 above that result in a change to the information and the changed information has an impact on decisions that have been or will be taken in respect of the Data Subject in question, the Company shall, if reasonably practicable, inform each person or body or Responsible Party to whom the personal information has been disclosed of those steps.

21.4 The Company shall notify a Data Subject, who has made a request in terms of paragraph 21.1 above, of the action taken in response to the request.

22. PROHIBITION ON PROCESSING OF SPECIAL PERSONAL INFORMATION BY THE COMPANY

22.1 The Company shall, subject to the provisions of section 27 of POPIA, not process personal information, referred to as "special personal information" concerning–

22.1.1 the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a Data Subject; or

22.1.2 the criminal behaviour of a Data Subject to the extent that such information relates to–

22.1.2.1 the alleged commission by a Data Subject of any offence; or

22.1.2.2 any proceedings in respect of any offence allegedly committed by a Data Subject or the disposal of such proceedings.

23. GENERAL AUTHORISATION CONCERNING SPECIAL PERSONAL INFORMATION

23.1 The prohibition on processing personal information, as referred to in paragraph 22 above and section 26 of POPIA, does not apply if the–

23.1.1 processing is carried out with the consent of a Data Subject referred to in section 26 of POPIA;

23.1.2 processing is necessary for the establishment, exercise or defence of a right or obligation in law;

23.1.3 processing is necessary to comply with an obligation of international public law;

23.1.4 processing is for historical, statistical or research purposes to the extent that–

23.1.4.1 the purpose serves a public interest and the processing is necessary for the purpose concerned; or

23.1.4.2 it appears to be impossible or would involve a disproportionate effort to ask for consent, and sufficient guarantees are provided for to ensure that the processing

does not adversely affect the individual privacy of the Data Subject to a disproportionate extent;

23.1.5 information has deliberately been made public by the Data Subject; or

23.1.6 provisions of section 28 to 33 of POPIA are, as the case may be, complied with.

23.2 The Information Regulator may, upon application by the Company and by notice in the *Gazette*, authorise the Company to process special personal information if such processing is in the public interest and appropriate safeguards have been put in place to protect the personal information of the Data Subject.

24. AUTHORISATION CONCERNING DATA SUBJECT'S RELIGIOUS OR PHILOSOPHICAL BELIEFS

24.1 The Company acknowledges that the prohibition on processing of special personal information concerning a Data Subject's religious or philosophical beliefs, as referred to in section 26 of POPIA, does not apply if the processing is carried out by–

24.1.1 spiritual or religious organisations, or independent sections of those organisations if–

24.1.1.1 the information concerns Data Subjects belonging to those organisations; or

24.1.1.2 it is necessary to achieve their aims and principles;

24.1.2 institutions founded on religious or philosophical principles with respect to their members or employees or other persons belonging to the institution, if it is necessary to achieve their aims and principles; or

24.1.3 other institutions: Provided that the processing is necessary to protect the spiritual welfare of the Data Subjects, unless they have indicated that they object to the processing.

24.2 In the cases referred to in paragraph 24.1.1 above, the prohibition does not apply to processing of personal information concerning the religion or philosophy of life of family members of the Data Subjects, if–

24.2.1 the association concerned maintains regular contact with those family members in connection with its aims; and

24.2.2 the family members have not objected in writing to the processing.

24.3 In the cases referred to in paragraphs 24.1 and 24.2 above, personal information concerning a Data Subject's religious or philosophical beliefs may not be supplied to third parties without the consent of the Data Subject.

25. AUTHORISATION CONCERNING DATA SUBJECT'S RACE OR ETHNIC ORIGIN

25.1 The Company acknowledges that the prohibition on processing personal information concerning a Data Subject's race or ethnic origin, as referred to in section 26 of POPIA, does not apply if the processing is carried out to–

25.1.1 identify Data Subjects and only when this is essential for that purpose; and

25.1.2 comply with laws and other measures designed to protect or advance persons, or categories of persons, disadvantaged by unfair discrimination.

26. AUTHORISATION CONCERNING DATA SUBJECT'S TRADE UNION MEMBERSHIP

26.1 The Company acknowledges that the prohibition on processing of special personal information concerning the trade union membership of an employee as Data Subject, as referred to in section 26 of POPIA, does not apply to the processing by the trade union to which the Data Subject belongs or the trade union federation to which that trade union belongs, if such processing is necessary to achieve the aims of the trade union or trade union federation.

26.2 In the cases referred to under paragraph 26.1 above, no personal information shall be supplied by the Company to third parties without the consent of the employee as Data Subject.

27. AUTHORISATION CONCERNING DATA SUBJECT'S POLITICAL PERSUASION

27.1 The Company acknowledges that the prohibition on processing of special personal information concerning a Data Subject's political persuasion, as referred to in section 26 of POPIA, does not apply to the processing by or for an institution, founded on political principles, of the personal information of–

27.1.1 its members or employees or other persons belonging to the institution, if such processing is necessary to achieve the aims or principles of the institution; or

27.1.2 a Data Subject if such processing is necessary for the purposes of–

27.1.2.1 forming a political party;

27.1.2.2 participating in the activities of, or engaging in the recruitment of members or canvassing supporters or voters for, a political party with the view to–

27.1.2.2.1 an election of the National Assembly or the provincial legislature, as regulated in terms of the Electoral Act, 1998 (Act No. 73 of 1998);

27.1.2.2.2 municipal elections as regulated in terms of the Local Government: Municipal Electoral Act, 2000 (Act No. 27 of 2000); or

27.1.2.2.3 a referendum as regulated in terms of the Referendums Act, 1983 (Act No. 108 of 1983); or

27.1.2.3 campaigning for a political party or cause.

27.2 In the cases referred to under paragraph 27.1 above, no personal information shall be supplied by the Company to third parties without the consent of the Data Subject.

28. AUTHORISATION CONCERNING DATA SUBJECT'S HEALTH OR SEX LIFE

28.1 The Company acknowledges that the prohibition on processing of special personal information concerning a Data Subject's health or sex life, as referred to in section 26 of POPIA, does not apply to the processing by–

28.1.1 medical professionals, healthcare institutions or facilities or social services, if such processing is necessary for the proper treatment and care of the Data Subject, or for the administration of the institution or professional practice concerned;

28.1.2 insurance companies, medical schemes, medical scheme administrators and managed healthcare organisations, if such processing is necessary for–

28.1.2.1 assessing the risk to be insured by the insurance company or covered by the medical scheme and where the Data Subject has not objected to the processing;

28.1.2.2 the performance of an insurance or medical scheme agreement; or

28.1.2.3 the enforcement of any contractual rights and obligations;

28.1.3 schools, if such processing is necessary to provide special support for pupils or making special arrangements in connection with their health or sex life;

28.1.4 any public or private body managing the care of a child if such processing is necessary for the performance of their lawful duties;

28.1.5 any public body, if such processing is necessary in connection with the implementation of prison sentences or detention measures; or

28.1.6 administrative bodies, pension funds, companies or institutions working for them, if such processing is necessary for–

28.1.6.1 implementation of the provisions of laws, pension regulations or collective agreements which create rights dependent on the health or sex life of the Data Subject; or

28.1.6.2 the reintegration of or support for workers or persons entitled to benefit in connection with sickness or work incapacity.

28.2 The information referred to in paragraph 28.1 above, shall only be processed by the Company subject to an obligation of confidentiality by virtue of office, employment, profession or legal provision, or established by a written agreement between the Company and the Data Subject.

28.3 If the Company is permitted to process information concerning a Data Subject's health or sex life in terms of paragraph 28.1 above, and is not subject to an obligation of confidentiality by virtue of office, profession or legal provision, it shall treat the information as confidential, unless the Company is required by law or in connection with their duties, to communicate the information to other parties who are authorised to process such information in accordance with paragraph 28.1 above.

28.4 The prohibition on processing any of the categories of special personal information referred to in section 26 of POPIA by the Company does not apply if it is necessary to supplement the processing of personal information concerning a Data Subject's health, as referred to under paragraph 28.1.1 above, with a view to the proper treatment or care of the Data Subject.

28.5 Personal information concerning inherited characteristics may not be processed in respect of a Data Subject from whom the information concerned has been obtained, unless–

28.5.1 a serious medical interest prevails; or

28.5.2 the processing is necessary for historical, statistical or research activity.

29. AUTHORISATION CONCERNING DATA SUBJECT'S CRIMINAL BEHAVIOUR OR BIOMETRIC INFORMATION

29.1 The prohibition on processing of special personal information by the Company concerning a Data Subject's criminal behaviour or biometric information, as referred to in section 26 of POPIA, does not apply if the processing is carried out by bodies charged by law with applying criminal law or by the Company which had obtained that information in accordance with the law.

29.2 The processing of information concerning employees of the Company shall take place in accordance with the rules established in compliance with labour legislation, and agreements concluded with employees in this regard.

29.3 The prohibition on processing any of the categories of special personal information referred to in section 26 of POPIA does not apply if such processing is necessary to supplement the processing of information on criminal behaviour or biometric information permitted by section 33 of POPIA.

30. GENERAL AUTHORISATION CONCERNING PERSONAL INFORMATION OF CHILDREN

30.1 The Company shall not process the personal information of children unless it is:

30.1.1 processed with the prior consent of a competent person;

30.1.2 necessary for the establishment, exercise or defence of a right or obligation in law;

30.1.3 necessary to comply with an obligation of international public law;

30.1.4 processed for historical, statistical or research purposes to the extent that–

30.1.4.1 the purpose serves a public interest and the processing is necessary for the purpose concerned; or

30.1.4.2 it appears to be impossible or would involve a disproportionate effort to ask for consent and sufficient guarantees are provided for to ensure that the processing does not adversely affect the individual privacy of the child to a disproportionate extent; or

30.1.5 personal information which has deliberately been made public by the child with the consent of a competent person.

30.2 The Company may, however, be authorised by the Information Regulator to process the personal information of children if the processing is in the public interest and appropriate safeguards have been put in place to protect the personal information of the child.

31. INFORMATION OFFICER

31.1 The Company has appointed an Information Officer and a deputy Information Officer, namely **Deon Beekhuizen** as Information Officer and **Daleen Pereira** as Deputy Information Officer.

31.2 The duties and responsibilities of the Information Officer include–

31.2.1 the encouragement of compliance by the Company, subject to the conditions for the lawful processing of personal information;

31.2.2 dealing with requests in general made to the Company pursuant to this Policy and Manual compiled in terms of PAIA and POPIA, respectively;

31.2.3 working with the Information Regulator in relation to investigations conducted pursuant to Chapter 6 of POPIA in relation to the Company;

31.2.4 otherwise ensuring compliance by the Company with the provisions of POPIA and PAIA; and

31.2.5 such duties and responsibilities as may be prescribed from time to time by the Information Regulator.

31.3 Information Officers shall take up their duties in terms of POPIA only after the Company has registered them with the Information Regulator.

31.4 Any power or duty conferred or imposed on an Information Officer by POPIA is also applicable to a Deputy Information Officer of the Company.

32. DIRECT MARKETING BY MEANS OF UNSOLICITED ELECTRONIC COMMUNICATIONS

32.1 The processing of personal information of a Data Subject by the Company and any of its employees and representatives for the purpose of direct marketing by means of any form of electronic communication, including automatic calling machines, facsimile machines, SMSs or e-mail, is prohibited unless the Data Subject (client, customer or potential client) –

32.1.1 has given his/her or its consent to the processing; or

32.1.2 is, subject to paragraph 33.3 below, an existing client or customer of the Company.

32.2 The Company shall approach a Data Subject–

32.2.1 whose consent is required in terms of paragraph 33.1.1 above; and

32.2.2 who had not previously withheld such consent,

only once in order to request the consent of that Data Subject.

32.2.3 whose consent is required, in the prescribed manner and form.

32.3 The Company shall only process the personal information of a Data Subject who is a customer or client of the Company in terms paragraph 33.1.2 above–

32.3.1 if the Company has obtained the contact details of the Data Subject in the context of the sale of a product or service;

32.3.2 for the purpose of direct marketing of the Company's own similar products or services; and

32.3.3 if the Data Subject has been given a reasonable opportunity to object, free of charge and in a manner free of unnecessary formality, to such use of his/her or its electronic details–

32.3.3.1 at the time when the information was collected; and

32.3.3.2 on the occasion of each communication with the Data Subject for the purpose of marketing if the Data Subject had not initially refused such use.

32.4 Any communication for the purpose of direct marketing must contain–

32.4.1 details of the identity of the sender or the person on whose behalf the communication has been sent; and

32.4.2 an address or other contact details to which the recipient may send a request that such communications cease.

32.5 **'Automatic calling machine'**, for purposes of paragraph 32.1 above, means a machine that is able to do automated calls without human intervention.

33. TRANSBORDER INFORMATION FLOWS

33.1 The Company shall not transfer personal information about a Data Subject to a third party who is in a foreign country unless–

33.1.1 the third party who is the recipient of the information is subject to a law, binding corporate rules or binding agreement which provide an adequate level of protection which–

33.1.1.1 effectively upholds principles for reasonable processing of the information that are substantially similar to the conditions for the lawful processing of personal information relating to a Data Subject who is a natural person and, where applicable, a juristic person; and

33.1.1.2 includes provisions that are substantially similar to this paragraph, relating to the further transfer of personal information from the recipient to third parties who are in a foreign country;

33.1.2 the Data Subject consents to the transfer;

33.1.3 the transfer is necessary for the performance of a contract between the Data Subject and the Company, or for the implementation of pre-contractual measures taken in response to the Data Subject's request;

33.1.4 the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the Company and a third party; or

33.1.5 the transfer is for the benefit of the Data Subject, and–

33.1.5.1 it is not reasonably practicable to obtain the consent of the Data Subject to that transfer; and

33.1.5.2 if it were reasonably practicable to obtain such consent, the Data Subject would be likely to give such consent.

34. ERASURE OF DATA AND RETURN OF DATA MEDIA

34.1 Employees are obliged, in terms of data protection provisions, to hand over or, by prior agreement, destroy all documents, compiled results of processing and use, and stored data that came into their possession. The same applies to test and rejected material.

34.2 Documentation and records that serve to verify mandated and proper personal information and data processing must be stored by employees in accordance with the respective storage periods. In order to disencumber themselves, employees may hand over such documentation to the Company.

34.3 Employees are obliged to implement technical and organisational measures communicated from time to time by the Company for protection of the Company's data stored on their servers or on the servers of affiliated companies.

35. CONFIDENTIALITY IN GENERAL

35.1 All information shall be considered confidential. Confidentiality protects information as assets from unauthorised disclosure. At no stage during the employment relationship may an employee disclose any information to any person inside or outside the Company. Any disclosure of information, irrespective of form, except where it is permitted, shall lead to disciplinary action.

35.2 Employees should never disclose any confidential information to any unauthorised person or third party about the Company, fellow employees, consultants, clients, customers, vendors, suppliers or competitors.

35.3 Employees should maintain the confidentiality of Company trade secrets and information. Trade secrets may include information regarding the development of systems, processes, products, know-how and technology. This also includes internal reports, policies, procedures or other internal business-related confidential communications referred to in general as **"confidential information"**.

35.4 Employees are obliged to report any breach or possible or suspected breach of this Policy immediately to their supervisor or manager.

36. TRAINING

36.1 Information security training shall be presented once a year for all employees working with personal and confidential information.

36.2 The Information Officer has the main responsibility of ensuring that training courses are held for each employee of the Company.

37. THE COMPANY'S POWERS GIVEN BY THE COMPANY AND EMPLOYEES' RIGHTS IN RESPECT OF INSTRUCTIONS

37.1 Personal information and data in the possession or control of the Company, shall be handled exclusively within the framework of this Policy and on the instruction of the Company. The Company reserves the right, within the framework of this Policy, to give instructions with regard to the type, scope and procedures of personal information and data processing and to specify more closely by means of individual instructions. Changes in the subject matter of the processing and changes in procedures with regard to personal information and data must be agreed mutually and documented.

37.2 Verbal instructions relating to any aspect regulated by this Policy shall be confirmed by the Company without delay in writing or per email.

37.3 In compliance with the respectively applicable provisions of POPIA, employees are obliged to inform the Company without delay if they believe an instruction infringes upon any personal information protection provisions. Employees are entitled to defer performance of the relevant instruction until such time as this has been confirmed or modified by the responsible person at the Company.

POLICY ISSUED BY:

NAME OF PERSON: _____

CAPACITY: _____

DATE: _____