COMPLIANCE MANUAL IN TERMS OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2014

INTERNAL POLICIES AND PROCEDURES

TABLE OF CONTENTS

POPIA INTERNAL COMPLIANCE MANUAL

1. PURPOSE AND USE OF INTERNAL COMPLIANCE MANUAL

1.1 The Constitution of the Republic of South Africa, 1996 recognizes that every Person has the right to privacy. In order to protect this right to privacy and specifically the Personal Information of Persons, the Protection of Personal Information Act 4 of 2013 was promulgated. The Company recognizes that it is a Responsible Party in terms of the Act and is therefore bound by the rules laid down for the Processing of Personal Information.

1.2 The purpose of this Compliance Manual is to lay down the internal policies and procedures adopted by the Company in order to comply with the rules and regulations for the Processing of Personal Information as provided for under the Act with the promulgated regulations and guidance notes.

1.3 This internal Compliance Manual must be read together with the PAIA Manual of the Company and will set out the more detailed internal rules and regulations to be followed by the Company and its Personnel.

1.4 The Company undertakes to use its best endeavors to comply with the Act and realizes that the protection of Personal Information is an ongoing process.

2. DEFINITIONS

For purposes of this Compliance Manual, the definitions as set out in the Company's PAIA Manual will also apply to this document.

3. GENERAL PRINCIPLES OF LAWFUL PROCESSING OF PERSONAL INFORMATION

3.1 The POPI Act sets forth 8 conditions[1] for the lawful Processing of Personal Information, namely:

3.1.1 **Condition 1: ACCOUNTABILITY**

[1] Section 4 of the POPI Act.

3.1.1.1 This condition entails that the Company, as Responsible Party, must ensure that the eight conditions and the measures that give effect to the conditions are complied with during the Processing of Personal Information under its control.

3.1.2 **Condition 2: PROCESSING LIMITATION**

3.1.2.1 The Company has to ensure that the following elements are complied with during Processing:

3.1.2.1.1 the lawfulness of the Processing[2] - the element of lawfulness means that the Responsible Party is prohibited from acting unlawfully in its collection of the Processing of the Personal Information;

3.1.2.1.2 minimality[3] - Personal Information may only be Processed if, given the purpose for which it is Processed, it is not excessive. The minimality condition ensures that only Personal Information which is appropriate for the purpose, is being collected;

3.1.2.1.3 Consent[4] - Personal Information may only be Processed if the Data Subject, or a Competent Person where the Data Subject is a Child, Consents to the Processing;

3.1.2.1.4 collection directly from the Data Subject[5] - Personal Information must be collected directly from the Data Subject, subject to certain exceptions when it is not necessary to collect the Personal Information from the Data Subject itself[6]. To this extent, Section 12(2)(f) of the POPI Act provides that direct collection is not necessary if it is not reasonably practical to do so.

3.1.3 **Condition 3 - PURPOSE SPECIFICATION**

3.1.3.1 This condition consists of three separate elements namely:

3.1.3.1.1 the collection for a specific purpose;

[2] Section 9 of the POPI Act.
[3] Section 10 of the POPI Act.
[4] Section 11 of the POPI Act.
[5] Section 12 of the POPI Act.
[6] Section 12(2) of the POPI Act.

3.1.3.1.2 that the Data Subject is aware of the purpose of collection;

3.1.3.1.3 the retention of Personal Information for no longer than the information may be required.

3.1.4 **Condition 4 - FURTHER PROCESSING LIMITATION**

3.1.4.1 A Responsible Party must restrict the Processing of Personal Information if:

3.1.4.1.1 its accuracy is contested by the Data Subject, for a period enabling the Responsible Party to verify the accuracy of the information;

3.1.4.1.2 the Responsible Party 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;

3.1.4.1.3 the Processing is unlawful, and the Data Subject opposes its destruction or deletion and requests the restriction of its use instead;

3.1.4.1.4 the Data Subject requests to transmit the personal data into another automated Processing system.

3.1.5 **Condition 5 - INFORMATION QUALITY**

3.1.5.1 The Company, as Responsible Party, has an obligation to ensure that the Personal Information under its control is:

3.1.5.1.1 complete;

3.1.5.1.2 accurate;

3.1.5.1.3 not misleading;

3.1.5.1.4 updated where necessary.

3.1.6 **Condition 6 - OPENNESS**

3.1.6.1 The "openness" condition requires that the Company, as Responsible Party, must maintain Process of all its Processing operations in terms of Section 14 or 15 of PAIA.

3.1.6.2 It also entails that the Data Subject is informed of the following:

3.1.6.2.1 the information being collected;

3.1.6.2.2 where the information is not collected from the Data Subject, the source from which it is collected;

3.1.6.2.3 the name and address of the Responsible Party;

3.1.6.2.4 the purpose for which the information is being collected;

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

3.1.6.2.6 the consequences of failure to provide the information;

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

3.1.6.2.8 the fact that, where applicable, the Responsible Party intends to transfer the information to a country other than South Africa or international organisation;

3.1.6.2.9 the level of protection afforded to the information by a country other than South Africa or international organisation;

3.1.6.2.10 the recipient or category of recipients of the information;

3.1.6.2.11 the nature or category of the information;

3.1.6.2.12 the right of access to the information collected;

3.1.6.2.13 the right to rectify the information collected;

3.1.6.2.14 the right to object to the Processing of Personal Information as referred to in Section 11(3) of POPI;

3.1.6.2.15 the right to lodge a complaint to the Information Regulator;

3.1.6.2.16 the contact details of the Information Regulator.

3.1.7 **Condition 7 - SECURITY SAFEGUARDS**

3.1.7.1 A Responsible Party must secure the integrity and confidentiality of Personal Information in its possession or under its control by taking:

3.1.7.1.1 appropriate measures;

3.1.7.1.2 reasonable technical measures;

3.1.7.1.3 organisational measures;

to prevent the unlawful access to the Personal Information of a Data Subject.

3.1.7.2 The Responsible Party must 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.

3.1.7.3 In order to prevent the unlawful Processing of Personal Information in the possession of the Responsible Party, the Responsible Party must take reasonable measures to:

3.1.7.3.1 identify all reasonably foreseeable internal and external risks to Personal Information in its possession or under its control;

3.1.7.3.2 establish appropriate safeguards against the risks identified;

3.1.7.3.3 maintain appropriate safeguards against the risks identified;

3.1.7.3.4 regularly verify that the safeguards are effectively implemented;

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

3.1.7.4 A Responsible Party must secure the integrity and confidentiality of Personal Information in its possession or under its control by taking the necessary appropriate, reasonable technical and organisational measures to prevent:

3.1.7.4.1 loss of Personal Information;

3.1.7.4.2 damage to Personal Information;

3.1.7.4.3 unauthorised destruction of Personal Information;

3.1.7.4.4 unlawful access to Personal Information;

3.1.7.4.5 unlawful Processing of Personal Information.

3.1.8 **Condition 8 - DATA SUBJECT PARTICIPATION**

3.1.8.1 A Data Subject, having provided adequate proof of identity, has the right to request from a Responsible Party the Process or a description of the Personal Information about the Data Subject held by the Responsible Party, including information about the identity of all Third Parties, or categories of Third Parties, who have, or have had, access to the information.

3.1.8.2 A Data Subject may, in the prescribed manner, request a Responsible Party to correct or delete Personal Information about that Data Subject in the Responsible Party's possession or under its control that is either inaccurate; irrelevant; excessive; out of date; incomplete; misleading; or obtained unlawfully.

4. THE APPOINTMENT OF AN INFORMATION OFFICER

4.1 The Company will ensure that at all times it has an appointed Information Officer who is registered with the Regulator. The Information Officer will be primarily responsible to ensure that the provisions of the POPI Act are complied with.

4.2 An Information Officer must take up his duties in terms of the POPI Act only after the Company has registered them with the Regulator. The Information Officer must complete and submit the registration form to the Regulator. The current Information Officer has been duly registered.

4.3 Should there be a change in Information Officer, the particulars must be updated internally and the new Information Officer registered with the Regulator and the PAIA Manual must be updated with the correct contact information.

4.4 Proper guidance and training must be provided to the Information Officer on a regular basis to ensure that the individual is aware and understands the conditions and measures required for the lawful Processing of Personal Information.

4.5 The Information Officer is responsible for implementing the policies and procedures laid down in this Compliance Manual.

4.6 The Company may also appoint a Deputy Information Officer to whom the responsibilities in terms of the POPI Act, as well as PAIA, will be delegated. The Deputy Information Officer will be afforded sufficient time, adequate resources and the financial means to devote to matters concerning POPI Act and PAIA. If a Deputy Information Officer is appointed, he will report to the Managing Director or Chief Executive Officer of the Company. Despite any designation of a Deputy Information Officer(s), an Information Officer retains the accountability and responsibility for the functions delegated to the Deputy Information Officer.

4.7 The Information Officer and Deputy Information Officer must be informed that the Regulator will make their contact details available on its website.

5. PERSONAL INFORMATION IMPACT ASSESSMENT

5.1 The Information Officer has performed an initial Personal Information Impact Assessment to determine whether adequate measures and standards exist in order to comply with the conditions for the lawful Processing of Personal Information. The details and outcome of this assessment must be stored as part of the Company's POPIA Compliance file.

5.2 A standard form Personal Information Impact Assessment is part of the Company's POPIA Compliance file and marked as Form B.

5.3 This Personal Information Impact Assessment must be conducted on an annual basis to identify which parts of the POPI Act is applicable to the Company, who the Data Subjects of the Company currently are, what information is collected and Processed and what measures have been taken and whether they are still

effective and what measures need to be taken to ensure lawful Processing and safeguarding of the information on an ongoing basis.

5.4 If the Personal Information Impact Assessment indicates any non-compliance with this Compliance Manual or the POPI Act, the Information Officer and the Company must take immediate steps to correct the non-compliance.

5.5 If the Personal Information Impact Assessment indicates new categories of Data Subjects or different information or Processing which is taking place in respect of Data Subjects, the PAIA Manual must be updated in accordance with the results of the impact assessment.

5.6 The outcome of the annual Personal Information Impact Assessment must be filed as part of the POPIA Compliance file of the Company as this will constitute the Record of the ongoing compliance initiatives taken by the Company.

6. GENERAL PRINCIPLES: THE RIGHTS OF DATA SUBJECTS

The Company notes that in terms of the POPI Act, all Data Subjects have certain specific and enforceable rights as set out in Clause 18.4 of the PAIA Manual.

7. GENERAL PRINCIPLES: PROCESSING OF PERSONAL INFORMATION OF DATA SUBJECTS

7.1 The Company notes that the Processing of Personal Information of a Data Subject is prohibited unless one of the grounds as set out in Clause 18.5 of the PAIA Manual is present.

7.2 The Company undertakes that it will only Process the Personal Information of a Child in accordance with the principles set out in Clause 18.6 of the PAIA Manual.

7.3 The Company notes that the POPI Act does not apply to the Processing of Personal Information:

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

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

7.3.3 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.

7.4 The Company will apply for and obtain prior authorisation from the Regulator, if necessary, as provided for in Clause 18.7 to 18.9 of the PAIA Manual.

8. SPECIFIC UNDERTAKINGS RELATING TO THE PROCESSING OF PERSONAL INFORMATION BY THE COMPANY

8.1 LAWFUL PROCESSING

The Company will only Process Personal Information in a lawful manner that does not infringe upon the privacy of the Data Subject.

The Company will only Process Personal Information of a Data Subject to enforce any right that the Company may have and will not sell such processed information of a Data Subject to any third party.

8.2 MINIMALITY OF COLLECTION OF DATA & COLLECTION OF INFORMATION FOR SPECIFIC PURPOSE

8.2.1 The Company will only Process data that it actually needs for the purposes of running the business, executing its contracts and protecting its legitimate interests. The Company will ensure that Personal Information collected is adequate, relevant and not excessive, when taking into account the specific purpose for which the information of that particular Data Subject is collected.

8.2.2 The type of Personal Information collected, and the purpose thereof, is stated in the PAIA Manual in Clauses 19.2 and 20.

8.2.3 As part of the annual Personal Information Impact Assessment, all Personal Information obtained per Data Subject will be evaluated against the purpose for which it is being Processed to identify whether it is adequate, relevant and not excessive. If found not to comply, the Personal Information will be destroyed in accordance with the principles contained later in this Compliance Manual. The PAIA Manual must be updated if the impact assessment indicates that other information is being collected or that the purpose for collection has changed.

8.2.4 The Company will always strive to collect Personal Information directly from the Data Subject concerned unless one of the following exclusions as set out in Clause 19.1.2 of the PAIA Manual is applicable.

8.3 CONSENT OF DATA SUBJECT

8.3.1 The Company is bound to obtain the Consent of a Data Subject to the Processing of Personal Information as laid down in Clause 21 of the PAIA Manual.

8.3.2 The Company has the following standard Consent forms as part of its POPIA Compliance file and will ensure that the relevant Data Subject signs the Consent form and that it be kept as part of the Company's POPIA Compliance file:

8.3.2.1 Client Consent form;

8.3.2.2 Prospective Employee Consent form;

8.3.2.3 Employee Consent form;

8.3.2.4 Supplier Consent form.

8.3.3 The Company will also ensure that it has a pop-up "cookie" notification on its website to inform users of the website of what Personal Information is being collected.

8.3.4 The Company will ensure that the website privacy policy (with comprehensive cookie policy) informing Data Subjects of their rights in terms of, amongst other things POPIA, is available on the website.

8.4 OBJECTION BY DATA SUBJECT TO PROCESSING OF PERSONAL INFORMATION

The process set out in Clause 22 of the PAIA Manual must be followed where a Data Subject objects to the Processing of Personal Information.

8.5 Retention of Information

8.5.1 The Company will follow the guidelines set out in Clause 23 of the PAIA Manual as to the retention of Personal Information.

8.5.2 Proof or confirmation of deletion or destruction will be filed in the POPIA Compliance file to indicate compliance with POPIA.

8.6 LIMITATIONS ON THE FURTHER PROCESSING OF INFORMATION

The Company will follow the guidelines as set out in Clause 24 of the PAIA Manual when considering whether to Process Personal Information further.

8.7 QUALITY OF INFORMATION

8.7.1 The Company will take reasonably practical steps to ensure that the Personal Information is complete, accurate, not misleading and updated when necessary.

8.7.2 The process set out in Clause 25.2 of the PAIA Manual must be followed when any Data Subject requests the correction or deletion of any Personal Information.

8.8 TRANSBORDER INFORMATION FLOWS

8.8.1 The Company will follow the guidelines set out in Clause 26 of the PAIA Manual relating to cross-border sharing of Personal Information.

8.8.2 During each annual Personal Information impact assessment, the Company will assess whether it still meets these guidelines and will update the PAIA Manual if any changes have occurred.

9. ACCESS TO INFORMATION BY DATA SUBJECT

The Company will follow the process as set out in Clause 27 of the PAIA Manual for any request to access for information by a Data Subject.

10. SAFETY MEASURES FOR THE PROTECTION OF PERSONAL INFORMATION

10.1 The Company must 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:

10.1.1 Loss of, damage to or unauthorised destruction of Personal Information; and

10.1.2 Unlawful access to or Processing of Personal Information.

10.2 The Company has performed a risk assessment which forms part of the POPIA Compliance file that identifies the internal and external risks to the Personal Information in the Company's possession or under its control. The risk assessment addresses where the information is stored, the safeguards protecting it and who has access thereto.

10.3 This risk assessment must be conducted on at least an annual basis to ensure that safeguards are still functional and to identify any new risks.

10.4 The safeguards implemented to address these risks are listed in the POPIA Compliance file and will be monitored on a regular basis and updated where deficiencies are identified.

10.5 The safeguards implemented by the Company must always be of a reasonable standard, taking into account the best industry practice, and must at least contain the following:

10.5.1 Physical access controls to information stored on paper;

10.5.2 Anti-virus programs;

10.5.3 Firewalls;

10.5.4 Password access controls to digital Process;

10.5.5 Remote destruction.

11. MAKING USE OF AN OPERATOR OR ACTING AS AN OPERATOR

11.1 If the Company makes use of Operators in the Processing of Personal Information, the following minimum standards must be adhered to:

11.1.1 A list of all Operators will be included in the POPIA Compliance file and updated at least every six months;

11.1.2 Each Operator must sign a POPIA service level agreement with the Company to ensure that the Operator establishes and maintains the same level of security measures that the Company does in

order to ensure the safeguarding of information. The service agreement must provide that the Operator must notify the Company immediately where there are reasonable grounds to believe that the Personal Information of a Data Subject has been accessed or acquired by any unauthorised Person. A standard form POPIA service level agreement is included under Point 13 of the POPIA Compliance file, and the Company will ensure that all Operators sign such agreement.

11.2 Where the Company acts as an Operator for another Responsible Party, it will comply with the following:

11.2.1 The Company will maintain a list of Responsible Parties for whom it acts as an Operator;

11.2.2 The Company will Process such information only with the knowledge or authorisation of the Responsible Party by way of a signed service agreement;

11.2.3 The Company will treat Personal Information which comes to its knowledge as confidential and shall not disclose it, unless required by law or in the course of the proper performance of our duties;

11.2.4 The Company will notify the Responsible Party immediately where there are reasonable grounds to believe that the Personal Information of a Data Subject has been accessed or acquired by any unauthorised Person;

11.2.5 The Company shall implement the same safeguards to the information Processed as it does where it acts as the Responsible Party in terms of the POPI Act.

12. INFORMATION BREACHES

The Company must follow the process as set out in Clause 30 of the PAIA Manual if any breach of Personal Information occurs.

13. DIRECT MARKETING

The Company must follow the process as set out in Clause 31 of the PAIA Manual for any Direct Marketing initiatives of the Company.

14. TRAINING OF COMPANY STAFF

14.1 The Company will provide training to all new employees and all existing employees as well as the Information Officer.

14.2 Training will be focused on ensuring that the staff knows what the Company's responsibilities are in terms of the POPI Act and its internal policies on how to meet these requirements. Training will also be conducted as necessary to inform the staff of any changes in POPIA and PAIA.

14.3 The Company will undertake training as follows:

14.3.1 For all new employees - a formal training session will be conducted within one month from the date on which they start to render services to the Company.

14.3.2 For existing employees - an initial training session will be done after adoption of this Compliance Manual and thereafter a refresher workshop will be conducted once per annum.

14.3.3 Information Officers - initial and annual training by way of a formal workshop will be conducted.

14.3.4 Changes in laws will be communicated as and when it comes into force.

14.4 Training Process will be kept as part of the POPIA Compliance file.

15. INFORMATION REGULATOR

15.1 The Company will report any breach of information to the Regulator as provided for in this Compliance Manual.

15.2 The Company takes note that any Person may submit a complaint to the Regulator alleging interference with the protection of the Personal Information of a Data Subject or non-compliance with the POPI Act. The Company further notes that, if it is aggrieved by the finding of any adjudicator, it can submit a complaint to the Regulator in the prescribed manner and form. These forms will form part of the Company's PAIA Manual privacy policy under Form F1 and F2.

16. PROMOTION OF ACCESS TO INFORMATION ACT

16.1 The Company will maintain a PAIA Manual which contains the following:

16.1.1 In general:

16.1.1.1 the postal and street addresses, phone and fax numbers and, if available, electronic mail address of the head of the body;

16.1.1.2 such other information as may be prescribed;

16.1.2 Insofar as PAIA is concerned:

16.1.2.1 a description of the guide of how to use PAIA as referred to in Section 10, if available, and how to obtain access to it;

16.1.2.2 the latest notice, if any, regarding the categories of Process of the body which are available without a Person having to request access in terms of PAIA;

16.1.2.3 a description of the Process of the body which are available in accordance with any other legislation;

16.1.2.4 sufficient detail to facilitate a request for access to a Process of the body, a description of the subjects on which the body holds Process and the categories of Process held on each subject;

16.1.3 Insofar as the Protection of Personal Information Act, 2013, is concerned:

16.1.3.1 the purpose of the Processing;

16.1.3.2 a description of the categories of Data Subjects and of the information or categories of information relating thereto;

16.1.3.3 the recipients or categories of recipients to whom the Personal Information may be supplied;

16.1.3.4 planned transborder flows of Personal Information; and

16.1.3.5 a general description allowing a preliminary assessment of the suitability of the information security measures to be implemented by the Responsible Party to ensure the confidentiality, integrity and availability of the information which is to be Processed.

16.2 The Manual must be made available:

16.2.1 on the website, if any, of the private body;

16.2.2 at the principal place of business of the private body for public inspection during normal business hours;

16.2.3 to any Person upon request and upon the payment of a reasonable amount; and

16.2.4 to the Information Regulator upon request.