THE PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013

&

THE PROMOTION OF ACCESS TO INFORMATION ACT 2 OF 2000

Compiled for:

Labour Life Consultancy (Pty) Ltd t/a Free State Polygraph and Verification

Contents

COMPANY PARTICULARS 3

COMPANY INFORMATION 3

INFORMATION OFFICER 3

DEPUTY INFORMATION OFFICER 3

ADMINISTRATION 4

INFORMATION OFFICER'S REGISTRATION FORM 5

REGISTRATION CERTIFICATE 6

DESIGNATION AND DELEGATION OF AUTHORITY TO THE DEPUTY INFORMATION OFFICER 7

AUTHORISATION OF INFORMATION OFFICER 8

TRAINING 9

POLICIES 10

GUIDELINES – APPOINTMENT OF DEPUTY INFORMATION OFFICER 11

DATA SUBJECT - PRIVACY NOTICE 15

PERSONAL INFORMATION PROTECTION POLICY 21

PERSONAL INFORMATION RETENTION POLICY 38

DATA BREACH POLICY 43

DATA SECURITY POLICY 47

DATA SUBJECT ACCESS REQUEST POLICY 54

POPIA FORMS 60

NOTIFICATION OF A SECURITY COMPROMISE IN TERMS OF SECTION 22 OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013) 61

FORM 1: OBJECTION TO THE PROCESSING OF PERSONAL INFORMATION 63

FORM 2: REQUEST FOR CORRECTION OR DELETION OF PERSONAL INFORMATION OR DESTROYING OR DELETION OF RECORD OF PERSONAL INFORMATION 64

FORM 4: APPLICATION FOR THE CONSENT OF A DATA SUBJECT FOR THE PROCESSING OF 65

PERSONAL INFORMATION FOR THE PURPOSE OF DIRECT MARKETING 65

DATA BREACH REGISTER 67

DATA BREACH REPORT FROM (INTERNAL USE) 69

PAIA MANUAL 72

COMPANY PARTICULARS

COMPANY INFORMATION

Company Name:	**Labour Life Consultancy (Pty) Ltd t/a Free State Polygraph and Verification**
Company Registration Number:	**2016/405893/07**
Nature of business:	**Labour Consultants**
Physical Address:	**77 First Street South** **Clocolan** **9735**
Postal Address:	**Po Box 13** **Clocolan** **9735**
E-Mail Address:	**admin@labourlife.co.za**
Telephone Number:	**0834642114**

INFORMATION OFFICER

Name:	**Jacob Coetzee**
Designation:	**Director**
Physical Address:	**77 First Street South** **Clocolan** **9735**
Postal Address:	**Po Box 13** **Clocolan** **9735**
E-Mail Address:	**jose@labourlife.co.za**
Telephone Number:	**0834642114**

DEPUTY INFORMATION OFFICER

Name:	**Kelly-Ann Roux**
Designation:	**Payroll Manager**
Physical Address:	**77 First Street South** **Clocolan** **9735**
Postal Address:	**Po Box 13** **Clocolan** **9735**
E-Mail Address:	**payroll@labourlife.co.za**
Telephone Number:	**0848292622**

ADMINISTRATION

INFORMATION OFFICER'S REGISTRATION FORM

REGISTRATION CERTIFICATE

DESIGNATION AND DELEGATION OF AUTHORITY TO THE DEPUTY INFORMATION OFFICER

AUTHORISATION OF INFORMATION OFFICER

TRAINING

POLICIES

GUIDELINES – APPOINTMENT OF DEPUTY INFORMATION OFFICER

1. RELEVANT DEFINITIONS

1.1. **"Body"** means public or private body;

1.2. **"Data Subject"** means the person to whom personal information relates.

1.3. **"Head"** of, or in relation to, a private body means-

a) in the case of a natural person, that natural person or any person duly authorised by that natural person;

b) in the case of a partnership, any partner of the partnership or any person duly authorised by the partnership;

c) in the case of a juristic person-

i. the chief executive officer or equivalent officer of the juristic person or any person duly authorised by that officer; or

ii. the person who is acting as such or any person duly authorised by such acting person.

1.4. **"Information Officer"**: of, or in relation to, a –

a) public body means an Information Officer or Deputy Information Officer as contemplated in terms of section 1 or 17; or

b) private body means the head of a private body as contemplated in section 1, of the Promotion of Access to Information Act.

1.5. **"Person"** means a natural person or a juristic person.

1.6. **"Personal Information"** – means information relating to an identifiable, living, natural person, identifiable, existing juristic person, including, but not limited to—

a) information relating to the race, gender, sex, national or social origin, language, age disability;

b) information relating to the education or medical or financial history of the person;

c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;

d) the biometric information of the person;

e) the personal opinion, views or preferences of the person;

f) 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;

g) the views or opinions of another individual about the person; and

h) 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.

1.7. **"Private Body"** means-

a) a natural person who carries or has carried on any trade, business or profession, but only in such capacity.

b) A partnership which carries or has carried on any trade, business or profession; or

c) Any former or existing juristic person.

1.8. **"Processing"** means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including—

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

b) dissemination by means of transmission, distribution or making available in any other form; or

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

1.9. **"Public Body"** means-

a) any department of state or administration in the national or provincial sphere of government or any municipality in the local sphere of government; or

b) any other functionary or institution when

i. exercising a power or performing a duty in terms of the Constitution or a provincial constitution; or

ii. exercising a public power or performing a public function in terms of any legislation.

1.10. **"Requester"**, in relation to-

a) a public body, means-

i. any person (other than a public body or an official thereof) making a request for access to a record of that public body; or

ii. a person acting on behalf of the person referred to in subparagraph (i) above;

b) a private body, means-

i. any person, including, but not limited to, a public body or an official thereof, making a request for access to a record of that private body; or

ii. a person acting on behalf of the person contemplated in subparagraph (i) above;

1.11 **''Responsible Party''** means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information;

1.12. The usage of the words **"responsible party"** and **"body"** interchangeable throughout this document depend on the contents of a specific paragraph.

2. INTRODUCTION

2.1. The Protection of Personal Information Act 4 of 2013 (POPIA) was enacted to promote the protection of personal information processed by public and private bodies and introduces-

a) minimum conditions for the lawful processing of personal information,

b) an obligation on Information Officers of public and private bodies to designate and delegate any power or duty to Deputy Information Officers; and

c) compulsory requirements for registration of Information Officers with the Information Regulator (Regulator).

2.2. The Information Officers are required, in terms of Section 55(2) of POPIA, to take up their duties only after being registered with the Regulator.

2.3. The Information Officers referred to in section 55(1) of POPIA are the same Information Officer referred to in sections 1 or 14 and 51 of PAIA.

2.4. The Information Officers of public or private bodies perform their duties and responsibilities in terms of both PAIA and POPIA.

3. PURPOSE

The purpose of this document is to provide guidance and procedures for the designation of Deputy Information Officers; and delegation of duties and responsibilities of the Information Officers to the Deputy Information Officers.

4. DUTIES OF THE INFORMATION OFFICER

4.1. Section 55(1) of POPIA sets out the duties and responsibilities of an Information Officer which include the encouragement of compliance by the body with the conditions for the lawful processing of personal information.

4.2. The additional duties and responsibilities of the Information Officers, in terms of regulation 4 of POPIA, are to ensure that-

a) a compliance framework is developed, implemented, monitored and maintained;

b) a personal information impact assessment is done to ensure that adequate measures and standards exist in order to comply with all the conditions for the lawful processing of personal information;
c) a manual is developed, monitored, maintained and made available as prescribed in sections 14 and 51 of PAIA, as amended;
d) internal measures are developed together with adequate systems to process requests for information or access thereto;
e) internal awareness sessions are conducted regarding the provisions of the Act, regulations made in terms of the Act, codes of conduct, or information obtained from the Regulator; and
f) upon request by any person, copies of the PAIA manual are provided to that person upon the payment of a fee to be determined by the Regulator from time to time.

4.3. The Regulator may request an Information Officer of a private body, in terms of section 83(4) of PAIA, to furnish to the Regulator with the information below.-
a) the number of requests for access received;
b) the number of requests for access granted in full;
c) the number of requests for access granted in terms of section 46;
d) the number of requests for access refused in full and refused partially and the number of times each provision of this Act was relied on to refuse access in full or partially;
e) the number of cases in which the periods stipulated in section 25(1) were extended in terms of section 26 (1);
f) the number of internal appeals lodged with the relevant authority and the number of cases in which, as a result of an internal appeal, access was given to a record;
g) the number of internal appeals which were lodged on the ground that a request for access was regarded as having been refused in terms of section 27;
h) the number of applications to a court which were lodged on the ground that an internal appeal was regarded as having been dismissed in terms of section 77 (7).

4.4. Registration of Information Officers with the Regulator is not only the prerequisite for Information Officer to take up their duties in terms of POPIA and PAIA, but is a compulsory requirement.

5. DELEGATION

5.1. An Information Officer(s) of both a public or private body must, subject to legislation and policies governing the employment of personnel of the body concerned, delegate powers or duties and responsibilities conferred or imposed on him or her to a Deputy Information Officer(s) of that body.

5.2. The delegation must be in writing, using the template below – "Delegation of Authority". An Information Officer should develop a framework for the delegation of his or her authority to a Deputy Information Officer.

5.3. The delegation of any powers or duties and responsibilities to a Deputy Information Officer does not prohibit an Information Officer from exercising the powers or performing the duty that he or she has delegated to a Deputy Information Officer.

5.4. Any power, duties and responsibilities delegated to a Deputy Information Officer(s) must be exercised or performed subject to such conditions as an Information Officer may considers necessary. Any conditions of delegation, as conferred on the Deputy Information Officer(s), must be reasonable and ensure sufficient and appropriate accessibility of a body by data subjects or requesters.

5.5. An Information Officer of a body must ensure that he or she reserves his or her rights in the aforesaid delegation to -

a) exercise the powers or to perform the duties and responsibilities concerned himself or herself; and
b) withdraw or amend the aforesaid delegation at any time.

5.6. An Information Officer must be aware that any right or privilege acquired, or any obligation or liability incurred because of a delegation of any powers, duties and responsibilities is not affected by any subsequent withdrawal or amendment of the decision to delegate.

5.7. To ensure a level of accountability by a designated Deputy Information Officer, bodies are encouraged to ensure that such duties and responsibilities or any power delegated to a Deputy Information Officer(s) is part of his or her job description.

5.8. Despite the above-mentioned designation a Deputy Information Officer(s), an Information Officer retains the accountability and responsibility for the functions delegated to the Deputy Information Officer.

DATA SUBJECT - PRIVACY NOTICE

1. BACKGROUND:

The Company understands that your privacy is important to you and that you care about how your personal information is used. We respect and value the privacy of all those that we have dealings with and use personal information in ways that are described here, and in a way that is consistent with our obligations and your rights under the law.

1.1. What Does This Notice Cover?

This Privacy Notice explains how we use your personal information: how it is collected, how it is held, and how it is processed. It also explains your rights under the law relating to your personal information.

1.2. What Is Personal information?

Personal information is defined by the Protection of Personal Information Act ("POPIA"), as 'any information relating to an identifiable living natural or existing juristic person'.
Personal information is, in simpler terms, any information about you that enables you to be identified. Personal information covers obvious information such as your name and contact details, but it also covers less obvious information such as identification numbers, electronic location data, and other online identifiers.
We process personal information by both automated (electronically) and non-automated means (paper based as part of a filing system).
The personal information that we use is set out in Part 5, below.

1.3. What Are My Rights?

Under POPIA, you have the right to have your personal information processed according to 8 processing conditions that are summarized as follows:

1.3.1. Condition 1 – Accountability.

We must ensure that the conditions set out in Chapter 3 of the Act and all the associated measures are complied with.

1.3.2. Condition 2 – Processing Limitation.

Personal information must be collected and processed lawfully in a reasonable manner that does not Infringe on your rights. Personal information may only be processed if it is adequate, relevant, and not excessive.
Personal information may only be processed if you consent thereto, alternatively where it is necessary to do so for the conclusion or performance of a contract, an obligation in terms of law, to protect your legitimate interest/s, or to pursue our legitimate interest/s.
Personal information must as far as possible be collected directly from you.

1.3.3. Condition 3 - Purpose Specification

Requires that personal information must be collected for a specific explicitly defined and lawful purpose related to a function or activity of ours. Such personal information may not be retained any longer than necessary for achieving the purposes for which the information was collected and/or subsequently processed.

1.3.4. Condition 4 - Further Processing Limitation

prohibits the further processing of your personal information unless such processing is compatible with the initial purpose of collecting the information.

1.3.5. Condition 5 - Information Quality

requires us to take reasonable, practicable steps to ensure that your personal information is complete, accurate, and not misleading. Such personal information must also be kept up to date, taking into consideration the purpose of the personal information.
The nature and purpose of your personal information will dictate as to how often such information must be updated.

1.3.6. Condition 6 - Openness

requires that we must, as far as it is practicable, inform you before your personal information is collected and the purpose of collecting and from where your personal information will be collected.
You are entitled to our details and must be made aware of the consequences of not disclosing personal information to us where it is required for a specific purpose.
You must also be made aware if your personal information is collected and processed as requirement established in law.
As per Section 72 of the Act, you will be advised if your personal information will be transferred across the borders of South Africa.

1.3.7. Condition 7 - Security Safeguards

requires that we must secure the integrity and confidentiality of your personal information by taking appropriate reasonable, technical, and organisational measures, to prevent the loss thereof or unlawful access thereto.

1.3.8. Condition 8 – Data Subject Participation

You have the right to establish whether your personal information is held by us and to have it corrected or destroyed if it is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or have been obtained unlawfully.

1.3.9. Other rights.

Your further have the following rights, which we will always work to uphold:

a) The right to be informed about our or collection and use of your personal information. This Privacy Notice should tell you everything you need to know, but you can always contact us to find out more or to ask any questions using the details in Part 11.
b) The right to access the personal information we hold about you. Part 10 will tell you how to do this.
c) The right to have your personal information rectified if any of your personal information held by us is inaccurate or incomplete. Please contact us using the details in Part 11 to find out more.
d) The right to be forgotten, in example the right to ask us to delete or otherwise dispose of any of your personal information that we hold. Please contact us using the details in Part 11 to find out more.
e) The right to restrict (i.e. prevent) the processing of your personal information.
f) The right to object to us using your personal information for a particular purpose or purposes.
g) The right to withdraw consent. This means that, if we are relying on your consent as the legal basis for using your personal information, you are free to withdraw that consent at any time.
h) The right to not have your personal information processed for the purposes of direct marketing by means of electronic communication without your consent.
i) Rights relating to automated decision-making and profiling.

It is important that your personal information is kept accurate and up to date. If any of the personal

information we hold about you changes, please keep us informed as long as we have that information.

Further information about your rights can also be obtained from the Information Regulator's Office at https://www.justice.gov.za/inforeg.

If you have any cause for complaint about our use of your personal information, you have the right to lodge a complaint with the Information Regulator's Office. We would welcome the opportunity to resolve your concerns ourselves, so please contact us first.

2. WHAT PERSONAL INFORMATION DO YOU COLLECT AND HOW?

We may collect and hold some or all of the personal information set out in the table below, using the methods also set out in the table. We do collect 'special personal information' where so required by law' and / or personal information relating to children, younger than 18 years of age, in so far as it relates to the children of our employees and for the purposes of medical insurance.

Special personal information may include information relating to race, ethnical origin, health, biometric information and criminal behaviour of a data subject.

The personal information of children may include the name, surname and date of birth or identity number of the child.

Information Collected	How We Collect the Personal Information
Identity Information including but not limited to identity numbers, drivers licences, passport numbers, names, surnames, company / entity names and registration details, vehicle registration numbers, CCTV footage, biometric information such as fingerprint images for access control.	As far as practicably possible directly from the data subject. If not practicable possible to obtain such information directly from you, we will obtain such personal information from third parties or public forums where you may have made your personal information deliberately public.
Contact and location information including but not limited to telephone and fax numbers, email addresses, physical addresses, postal addresses, geographical location data.	As far as practicably possible directly from the data subject. If not practicable possible to obtain such information directly from you, we will obtain such personal information from third parties or public forums where you may have made your personal information deliberately public.
Business information including but not limited to ownership, shareholding, job titles, professions, email communication of an implicit or explicit private and confidential nature, affiliations, products, services, statutory registration information.	As far as practicably possible directly from the data subject. If not practicable possible to obtain such information directly from you, we will obtain such personal information from third parties or public forums where you may have made your personal information deliberately public.
Payment information including but not limited to transaction history, bank statements, invoices, credit notes, credit / debit card details, bank account numbers, credit ratings.	As far as practicably possible directly from the data subject. If not practicable possible to obtain such information directly from you, we will obtain such personal information from third parties or public forums where you may have made your personal information deliberately public. Banks and credit rating / consumer data verification agencies.

Profile information including but not limited to preferences, customer profiles, transaction history, etc.	As far as practicably possible directly from the data subject. If not practicable possible to obtain such information directly from you, we will obtain such personal information from third parties or public forums where you may have made your personal information deliberately public.
Data from third parties including the verification of information, consumer profiles, etc.	As far as practicably possible directly from the data subject. If not practicable possible to obtain such information directly from you, we will obtain such personal information from third parties or public forums where you may have made your personal information deliberately public.

3. HOW DO YOU USE MY PERSONAL INFORMATION?

Under POPIA, we must always have a lawful basis for using personal information. We may use your personal information for one or all of the following purposes:

- The administration of our business.
- Supplying our products and / or services to you.
- Managing payments for our products and / or services.
- Personalising and tailoring our products and / or services for you.
- Communicating with you.
- Supplying you with information by electronic communication if you have agreed thereto (you may opt-out at any time by using the details in Part 11.
- With your permission we may also use your personal information for marketing purposes, which may include contacting you by email **and / or** telephone **and / or** text message with information, news, and offers on our products and / or services. You will not be sent any unlawful marketing or spam. We will always work to fully protect your rights and comply with our obligations under POPIA, and you will always have the opportunity to opt-out.

We will only use your personal information for the purpose(s) for which it was originally collected unless we reasonably believe that another purpose is compatible with that or those original purpose(s) and need to use your personal information for that purpose. If we do use your personal information in this way and you wish us to explain how the new purpose is compatible with the original, please contact us using the details in Part 11.

If we need to use your personal information for a purpose that is unrelated to, or incompatible with, the purpose(s) for which it was originally collected, we will inform you and explain the legal basis which allows us to do so or obtain permission from you to do so.

In some circumstances, where permitted or required by law, we may process your personal information without your knowledge or consent. This will only be done within the bounds of POPIA and your legal rights.

4. HOW LONG WILL YOU KEEP MY PERSONAL INFORMATION?

We will not keep your personal information for any longer than is necessary in light of the reason(s) for which it was first collected. Your personal information will therefore be kept for:

- as long as it serves the purpose it was collected and intended for,

- such periods as prescribed in any legislation applicable to our business,
- any period agreed to in a contract,
- the purposes of fulfilment of a contract, or
- any period you may have agreed to.

5. HOW AND WHERE DO YOU STORE OR TRANSFER MY PERSONAL INFORMATION?

We will endeavour to store your personal information in South Africa. This means that it will be fully protected under POPIA.

We may however transfer your personal information across the borders of South Africa for the purposes of storage, performance of a contract, an obligation in terms of international law or for internal purposes. These are referred to as "third countries". We will take additional steps in order to ensure that your personal information is treated just as safely and securely as it would be within South Africa and under POPIA by administering contracts and / or service agreements which ensure the same levels of personal information protection that apply under POPIA.

The security of your personal information is essential to us, and to protect your information, we take a number of important measures, including the following:

- Limiting access to your personal information to those employees, agents, contractors, and other third parties with a legitimate need to know and, where applicable, ensuring that they are subject to duties of confidentiality.
- Procedures for dealing with data breaches (the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, your personal information) including notifying you and the Information Regulator's Office where we are legally required to do so.
- We have identified all reasonable and foreseeable internal and external risks and introduced safeguards to mitigate such risks.
- Continuous maintenance and updating of such safeguards to secure your personal information.

6. DO YOU SHARE MY PERSONAL INFORMATION?

We will not share any of your personal information with any third parties for any purposes, subject to the following exception/s.

- For the purposes of *inter alia* fulfilment of an application, contract, rendering of a service or goods.
- If we sell, transfer, or merge parts of our business or assets, your personal information may be transferred to a third party. Any new owner of our business may continue to use your personal information in the same way(s) that we have used it, as specified in this Privacy Notice.
- In some limited circumstances, we may be legally required to share certain personal information, which might include yours, if we are involved in legal proceedings or complying with legal obligations, a court order, or the instructions of a government authority.
- We may share your personal information with other companies in our group which may include our holding company and its subsidiaries.

If any of your personal information is shared with a third party, as described above, we will take reasonable steps to ensure that your personal information is handled safely, securely, and in accordance with your rights.

7. OPERATORS:

We may make use of third-party service providers to process personal information on our behalf. To protect such personal information, we will enter into a formal written agreement with the service provider. In terms of such agreement the service provider will be required to process personal

information in accordance with conditions as prescribed by us, including measures to protect the security and integrity for such personal information.

8. HOW CAN I ACCESS MY PERSONAL INFORMATION?

If you want to know what personal information we have about you, you can ask us for details of that personal information and for a copy of it (where any such personal information is held). This is known as a Subject Access Request ("SAR").

All SARs should be made in writing and sent to the email or postal addresses shown in Part 11. To make this as easy as possible for you, a Subject Access Request Form is available for you to use (SAR Form 1). You do not have to use this form, but it is the easiest way to tell us everything we need to know to respond to your request as quickly as possible.

There may be a fee charged for a Subject Access Request, especially if your request is 'manifestly unfounded or excessive' (for example, if you make repetitive requests) a fee may be charged to cover our administrative costs in responding.

We will respond to your data subject access request within one month. Normally, we aim to provide a complete response, including a copy of your personal information within that time. In some cases, however, particularly if your request is more complex, more time may be required up to a maximum of three months from the date we receive your request. You will be kept fully informed of our progress.

9. CHANGES TO THIS PRIVACY NOTICE

We may change this Privacy Notice from time to time. This may be necessary, for example, if the law changes, or if we change our business in a way that affects personal information protection.

Any changes will be made available on our company website.

PERSONAL INFORMATION PROTECTION POLICY

1. Introduction

1.1. This Policy sets out the obligations of the Company regarding the protection of personal information and the rights of employees, customers, business contacts, etc. ("data subjects") in respect of their personal information under The Protection of Personal Information Act or "POPIA". "The Protection of Personal Information Act" means legislation and regulations in force from time to time regulating the use of personal information.

1.2. This Policy sets the Company's obligations regarding the collection, processing, transfer, storage, and disposal of personal information. The procedures and principles set out herein must be followed at all times by the Company, its employees, agents, contractors, or other parties working on behalf of the Company.

2. Definitions

"consent"	means any voluntary, specific and informed expression of will in terms of which permission is given to the processing of personal information;
"responsible party"	means the natural or legal person or organisation which, alone or jointly with others, determines the purposes and means of the processing of personal information. For the purposes of this Policy, the Company is the responsible party for all personal information relating to data subjects such as employees, customers, business contacts, etc. used in our business for our commercial purposes;
"operator"	means a natural or legal person or organisation which processes personal information on behalf of a responsible party;
"data subject"	means a living identifiable natural person or existing juristic person about whom the Company holds personal information;
"personal information"	Means any information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to— (a) information relating to the race, gender, sex, pregnancy, marital status, nationality, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person; (b) information relating to the education or the medical, financial, criminal or employment history of the person; (c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person; (d) the biometric information of the person; (e) the personal opinions, views or preferences of the person; (f) 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; (g) the views or opinions of another individual about the person; and (h) 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;
"personal information breach"	means a breach of security leading to the accidental or unlawful disclosure of, access to, or use of personal information under the control of the Company;
"processing"	means any operation or set of operations performed on personal information or sets of personal information, whether or not by automated means, such as but not limited to the collection, receipt, recording, organisation, structuring, storage, adaptation / alteration, retrieval, use, disclosure by transmission/dissemination or otherwise making available, alignment, merging, linking/combining, restriction, erasure or destruction thereof.
"de-identify"	means to delete any information that— (a) identifies the data subject; (b) can be used or manipulated by a reasonably foreseeable method to identify the data subject; or (c) can be linked by a reasonably foreseeable method to other information that identifies the data subject.
"special personal information"	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 (b) the criminal behaviour of a data subject to the extent that such information relates to— (i) the alleged commission by a data subject of any offence; or (ii) any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

3. Scope

3.1. The Company is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal information, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

3.2. The Company's Information Officer is the person at the head of the Company or the person acting in that position or the person duly appointed by the person at the head of the business. The Information Officer is responsible for administering this Policy and for developing and implementing any applicable related policies, procedures, and/or guidelines.

3.3. The Company's Information Officer has appointed Deputy Information Officers that will assist him/her with ensuring compliance with the Protection of Personal Information Act. The most recent details of the Information Officer and appointed deputies can be obtained from the Human Resources Department.

3.4. All employees that are appointed in positions with an inherent function of the supervision of others and/or performance of a department/division/unit are responsible for ensuring that all employees, agents, contractors, or other parties working on behalf of the Company comply with this Policy and, where applicable, must implement such practices, processes, controls, and training as are reasonably necessary to ensure such compliance.

3.5. Any questions relating to this Policy or to POPIA should be referred to the Information Officer or any of the Deputy Information Officers.

4. The Protection of Personal information Principles

4.1. This Policy aims to ensure compliance with POPIA and sets out the following principles with which any party handling personal information must comply with. Responsible Parties are

responsible for, and must be able to demonstrate, such compliance.

4.2. All personal information must be:

a) processed lawfully, fairly, and in a transparent manner in relation to the data subject;
b) collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest for historical, research or statistical purposes shall not be considered to be incompatible with the initial purposes;
c) adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed;
d) accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal information that is inaccurate, having regard to the purposes for which it is processed, is erased/destroyed, or rectified without delay;
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal information is processed. Personal information may be stored for longer periods insofar as the personal information will be processed solely for archiving purposes in the public interest such as for historical, statistical or research purposes, subject to implementation of the appropriate safeguards to prevent such records from being used for any other purpose;
f) processed in a manner that ensures appropriate security of the personal information, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

5. The Rights of Data Subjects

POPIA sets out the following key rights applicable to data subjects:

a) The right to be informed;
b) the right of access;
c) the right to rectification;
d) the right to erasure (also known as the 'right to be forgotten');
e) the right to restrict processing;
f) the right to object; and
g) rights with respect to automated decision-making and profiling
h) rights with respect to direct marketing using electronic communication as medium.

6. Lawful, Fair, and Transparent Data Processing

POPIA seeks to ensure that personal information is processed lawfully without adversely affecting the rights of the data subject. Specifically, the processing of personal information shall be lawful if at least one of the following applies:

a) the data subject has given consent to the processing of their personal information for one or more specific purposes;
b) the processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract;
c) the processing is necessary for compliance with a legal obligation to which the responsible party is subject;
d) the processing is necessary to protect the legitimate interests of either the data subject, the responsible party or a third party to whom such information is supplied; or
e) the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the responsible party; or
f) If the personal information in question is special category personal information (also known as

"special personal information"), at least one of the following conditions must be met:

I. the data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless the law prohibits them from doing so);
II. the processing is necessary for the purpose of establishment, exercise or defence of a right or obligation in law;
III. processing is required to serve an obligation in pubic or international law;
IV. the processing relates to special personal information which is deliberately made public by the data subject;
V. the processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity;
VI. the processing is authorized by the Information Regulator upon successful application; or
VII. the processing is necessary for archiving purposes in the public interest for historical, research or statistical purposes.

7. Consent

If consent is relied upon as the lawful basis for collecting, holding, and/or processing personal information, the following shall apply:

a) Consent is a clear indication, as far as possible in writing, by the data subject that they agree to the processing of their personal information. Silence, pre-ticked boxes, or inactivity do not amount to consent.
b) Where consent is given in a document which includes other matters, the section dealing with consent must be kept clearly separate from such other matters.
c) Data subjects are free to withdraw consent at any time and it must be made easy for them to do so. If a data subject withdraws consent, their request must be honoured promptly, unless such withdrawal of consent will significantly adversely affect the responsible party.
d) If personal information is to be processed for a different purpose that is incompatible with the purpose or purposes for which that personal information was originally collected that was not disclosed to the data subject when they first provided their consent, consent to the new purpose or purposes may need to be obtained from the data subject.
e) If special personal information is processed, the Company shall normally rely on a lawful basis other than explicit consent. However, if explicit consent is relied upon, the data subject must do so in writing.
f) In all cases where consent is relied upon as the lawful basis for collecting, holding, and/or processing personal information, records must be kept of all consents obtained in order to ensure that the Company can demonstrate its compliance with consent requirements.

8. Specified, Explicit, and Legitimate Purposes

8.1. The Company collects and processes the personal information set out in Part 23 of this Policy. This includes:
   a) personal information collected directly from data subjects; or
   b) personal information obtained from third parties.
8.2. The Company only collects, processes, and holds personal information for the specific purposes set out in Part 23 of this Policy (or for other purposes expressly permitted by POPIA).
8.3. Data subjects must be kept informed at all times of the purpose or purposes for which the Company uses their personal information. Please refer to Part 15 for more information on keeping data subjects informed.

9. Adequate, Relevant, and Limited Processing

9.1. The Company will only collect and process personal information for and to the extent necessary

for the specific purpose or purposes of which data subjects have been informed (or will be informed) as under Part 8, above, and as set out in Part 23, below.

9.2. Employees, agents, contractors, or other parties working on behalf of the Company may collect personal information only to the extent required for the performance of their job duties and only in accordance with this Policy. Excessive personal information must not be collected.

9.3. Employees, agents, contractors, or other parties working on behalf of the Company may process personal information only when the performance of their job duties requires it. Personal information held by the Company cannot be processed for any unrelated reasons.

10. Accuracy of Personal Information / Keeping Up to Date

10.1. The Company shall ensure that all personal information collected, processed, and held by it is kept accurate and up to date. This includes, but is not limited to, the rectification of personal information at the request of a data subject, as set out in Part 17, below.

10.2. The accuracy of personal information shall be checked when it is collected and, as determined by each Departmental Head, as and when required, having due regard to the nature and purpose of the personal information.

10.3. If any personal information is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

11. Retention of Personal Information

11.1. The Company shall not keep personal information for any longer than is necessary in light of the purpose or purposes for which that personal information was originally collected, held, and processed.

11.2. When personal information is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

11.3. For full details of the Company's approach to data retention, including retention periods for specific personal information types held by the Company, please refer to our Personal Information Retention Policy.

12. Secure Processing

12.1. The Company shall ensure that all personal information collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. Further details of the technical and organisational measures which shall be taken are provided in Parts 25 to 30 of this Policy.

12.2. All technical and organisational measures taken to protect personal information shall be regularly reviewed and evaluated to ensure their ongoing effectiveness and the continued security of personal information.

12.3. Data security must be maintained at all times by protecting the confidentiality, integrity, and availability of all personal information as follows:

a) only those with a genuine need to access and use personal information and who are authorised to do so may access and use it;

b) personal information must be accurate and suitable for the purpose or purposes for which it is collected, held, and processed; and

c) authorised users must always be able to access the personal information as required for the authorised purpose or purposes.

13. Accountability and Record-Keeping

13.1. The Information Officer is responsible for administering this Policy and for developing and implementing any applicable related policies, procedures, and/or guidelines.

13.2. The Company shall follow a "privacy by design" approach at all times when collecting,

holding, and processing personal information. POPIA Impact Assessments shall be conducted if any processing presents a significant risk to the rights of data subjects (please refer to Part 14 for further information).

13.3. All employees, agents, contractors, or other parties working on behalf of the Company shall be given appropriate training in the protection of personal information, addressing the relevant aspects of POPIA, this Policy, and all other applicable Company policies.

13.4. The Company's the protection of personal information compliance shall be regularly reviewed and evaluated by means of POPIA Audits.

13.5. The Company shall keep written internal records of all personal information collection, holding, and processing, which shall incorporate the following information:

a) the name and details of the Company, its Information Officer, and any applicable operators with whom personal information is shared;
b) the purposes for which the Company collects, holds, and processes personal information;
c) the Company's legal basis or bases (including, but not limited to, consent, the mechanism(s) for obtaining such consent, and records of such consent) for collecting, holding, and processing personal information;
d) details of the categories of personal information collected, held, and processed by the Company;
e) details of any transfers of personal information outside of South Africa including security safeguards;
f) details of how long personal information will be retained by the Company (please refer to the Company's Personal Information Retention Policy);
g) details of personal information storage, including location(s);
h) detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of personal information.

14. The POPIA Impact Assessments and Privacy by Design

14.1. In accordance with the privacy by design principles, the Company shall carry out POPIA Impact Assessments for any and all new projects and/or new uses of personal information which involve the use of new technologies and where the processing involved is likely to result in a high risk to the rights of data subjects.

14.2. The principles of privacy by design should be followed at all times when collecting, holding, and processing personal information. The following factors should be taken into consideration:

a) the nature, scope, context, and purpose or purposes of the collection, holding, and processing;
b) the state of the art of all relevant technical and organisational measures to be taken;
c) the cost of implementing such measures; and
d) the risks posed to data subjects and to the Company, including their likelihood and severity.

14.3. The protection of POPIA Impact Assessments shall be overseen by the Information Officer or a Deputy Information Officer and shall address the following:

a) the type(s) of personal information that will be collected, held, and processed;
b) the purpose(s) for which personal information is to be used;
c) the Company's objectives;
d) how personal information is to be used;
e) the parties (internal and/or external) who are to be consulted;
f) the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;
g) risks posed to data subjects;

h) risks posed both within and to the Company; and
i) proposed measures to minimise and handle identified risks.

15. Keeping Data Subjects Informed

15.1. The Company shall provide the information set out in Part 15.2 to every data subject:
a) where personal information is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and
b) where personal information is obtained from a third party, the relevant data subjects will be informed of its purpose:
c) if the personal information is used to communicate with the data subject, when the first communication is made; or
d) if the personal information is to be transferred to another party, before that transfer is made; or
e) as soon as reasonably possible and preferably not more than one month after the personal information is obtained.

15.2. The following information shall be provided in the form of a privacy notice:
a) details of the Company including, but not limited to, contact details, and the names and contact details of any applicable representatives and its Information Officer;
b) the purpose(s) for which the personal information is being collected and will be processed (as detailed in Part 23 of this Policy);
c) where applicable, the legitimate interests upon which the Company is justifying its collection and processing of the personal information;
d) where the personal information is to be transferred to a third party that is located outside of South Africa, details of that transfer, including but not limited to the safeguards in place (see Part 30 of this Policy for further details);
e) details of the data subject's rights under POPIA;
f) details of the data subject's right to withdraw their consent to the Company's processing of their personal information at any time;
g) details of the data subject's right to complain to the Information Regulator's;
h) details of any automated decision-making or profiling that will take place using the personal information, including information on how decisions will be made, the significance of those decisions, and any consequences.

16. Data Subject Access

16.1. Data subjects may make subject access requests ("SARs") at any time to find out more about the personal information which the Company holds about them, what it is doing with that personal information, and why.

16.2. Data subjects wishing to make a SAR should do using a Subject Access Request Form, sending the form to the Company's Information Officer

16.3. Responses to SARs must normally be made within one month of receipt, however, this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.

16.4. All SARs received shall be handled by the Company's Information Officer and in accordance with the Company's Data Subject Access Request Policy & Procedure.

16.5. The Company may charge a reasonable fee for the handling of normal SARs. The Company reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

17. Rectification of Personal information

17.1. Data subjects have the right to require the Company to rectify any of their personal information that is inaccurate or incomplete.

17.2. The Company shall rectify the personal information in question, and inform the data subject of that rectification, within one month of the data subject informing the Company of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

17.3. The Company may decline a data subject's request for personal information to be corrected and will keep a record of such request and the basis for declining the application.

18. Erasure of Personal information

18.1. Data subjects have the right to request that the Company erases the personal information it holds about them in the following circumstances:

a) it is no longer necessary for the Company to hold that personal information with respect to the purpose(s) for which it was originally collected or processed;

b) the data subject wishes to withdraw their consent to the Company holding and processing their personal information;

c) the data subject objects to the Company holding and processing their personal information (and there is no overriding legitimate interest to allow the Company to continue doing so) (see Part 20 of this Policy for further details concerning the right to object);

d) the personal information has been processed unlawfully;

e) the personal information needs to be erased in order for the Company to comply with a particular legal obligation.

18.2. Unless the Company has reasonable grounds to refuse to erase personal information, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

19. Restriction of Personal information Processing

Data subjects may request that the Company ceases processing the personal information it holds about them. If a data subject makes such a request, the Company shall retain only the amount of personal information concerning that data subject (if any) that is necessary to ensure that the personal information in question is not processed further.

20. Objections to Personal information Processing

20.1. Data subjects have the right to object to the Company processing their personal information based on legitimate interests or for direct marketing.

20.2. Where a data subject objects to the Company processing their personal information based on its legitimate interests, the Company shall cease such processing immediately, unless it can be demonstrated that the Company's legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.

20.3. Where a data subject objects to the Company processing their personal information for direct marketing purposes, the Company shall cease such processing promptly.

21. Automated Processing, Automated Decision-Making, and Profiling

n/a

22. Direct Marketing

22.1. The Company is subject to certain rules and regulations when marketing its products and/or services.

22.2. The prior consent of data subjects is required for electronic direct marketing including email, text messaging, and automated telephone calls subject to the following limited exception:

a) The Company may send marketing text messages or emails to a customer provided that that customer's contact details have been obtained in the course of a sale, the marketing relates to similar products or services, and the customer in question has given permission to the Company to do so. Further to this, the customer is given the opportunity to opt-out of marketing in every subsequent communication from the Company.

22.3. Direct marketing to data subjects, except as provided for in Part 22.2(a) above, may only take place upon being presented with written consent from the data subject. The Direct Marketing Consent From is to be used for this purpose.

22.4. The right to object to direct marketing shall be explicitly offered to data subjects in a clear and intelligible manner and must be kept separate from other information in order to preserve its clarity.

22.5. If a data subject objects to direct marketing, their request must be complied with promptly. A limited amount of personal information may be retained in such circumstances to the extent required to ensure that the data subject's marketing preferences continue to be complied with.

23. Personal information Collected, Held, and Processed

The following personal information is collected, held, and processed by the Company (for details of data retention, please refer to the Company's Personal Information Retention Policy):

Information	How We Collect the Personal Information
Identity Information including but not limited to identity numbers, drivers licences, passport numbers, names, surnames, company / entity names and registration details, vehicle registration numbers, CCTV footage, biometric information such as fingerprint images for access control.	As far as practicably possible directly from the data subject. If not practicable possible to obtain such information directly from you, we will obtain such personal information from third parties or public forums where you may have made your personal information deliberately public.
Contact and location information including but not limited to telephone and fax numbers, email addresses, physical addresses, postal addresses, geographical location data.	As far as practicably possible directly from the data subject. If not practicable possible to obtain such information directly from you, we will obtain such personal information from third parties or public forums where you may have made your personal information deliberately public.
Business information including but not limited to ownership, shareholding, job titles, professions, email communication of an implicit or explicit private and confidential nature, affiliations, products, services, statutory registration information.	As far as practicably possible directly from the data subject. If not practicable possible to obtain such information directly from you, we will obtain such personal information from third parties or public forums where you may have made your personal information deliberately public.
Payment information including but not limited to transaction history, bank statements, invoices, credit notes, credit / debit card details, bank account numbers, credit ratings.	As far as practicably possible directly from the data subject. If not practicable possible to obtain such information directly from you, we will obtain such personal information from third parties or public

	forums where you may have made your personal information deliberately public. Banks and credit rating / consumer data verification agencies.
Profile information including but not limited to preferences, customer profiles, transaction history, etc.	As far as practicably possible directly from the data subject. If not practicable possible to obtain such information directly from you, we will obtain such personal information from third parties or public forums where you may have made your personal information deliberately public.
Data from third parties including the verification of information, consumer profiles, etc.	As far as practicably possible directly from the data subject. If not practicable possible to obtain such information directly from you, we will obtain such personal information from third parties or public forums where you may have made your personal information deliberately public.

24. Data Security - Transferring Personal information and Communications

The Company shall ensure that the following measures are taken with respect to all communications and other transfers involving personal information:

a) All emails containing personal information must be encrypted
b) All emails containing personal information must be marked "confidential";
c) Personal information may not be transmitted over a public wireless network;
d) Personal information contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted by i.e., emptying the "Trash" or "Deleted Items" folders associated with an email address
e) Where personal information is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;
f) Where personal information is to be transferred in hardcopy form it should be passed directly to the recipient or sent using Company authorised delivery services
g) All personal information to be transferred physically, whether in hardcopy form or on removable electronic media shall be transferred in a suitable container marked "confidential";

25. Data Security – Storage

The Company shall ensure that the following measures are taken with respect to the storage of personal information:

a) All electronic copies of personal information should be stored securely using passwords and data encryption;
b) All hardcopies of personal information, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar;
c) All personal information stored electronically should be backed up frequently with backups stored onsite/offsite as applicable. All backups should be encrypted;
d) No personal information should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to the Company or otherwise without the formal written approval of the Information Officer and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is

given, and for no longer than is absolutely necessary;

e) No personal information should be transferred to any device personally belonging to an employee, agent, contractor, or other party working on behalf of the Company and personal information may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the Protection of Personal Information Act (which may include demonstrating to the Company that all suitable technical and organisational measures have been taken);

26. Data Security – Disposal

When any personal information is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and/or disposed of. For further information on the deletion and disposal of personal information, please refer to the Company's Personal Information Retention Policy.

27. Data Security - Use of Personal information

The Company shall ensure that the following measures are taken with respect to the use of personal information:

a) No personal information may be shared informally and if an employee, agent, contractor, or other party working on behalf of the Company requires access to any personal information that they do not already have access to, such access should be formally requested from the Information Officer;

b) No personal information may be transferred to any employee, agent, contractor, or other party, whether such parties are working on behalf of the Company or not, without the authorisation of the Information Officer;

c) Personal information must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, contractors, or other parties at any time;

d) If personal information is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it;

e) Where personal information held by the Company is used for marketing purposes, the Company shall ensure that the appropriate consent is obtained and that no data subjects have opted out;

28. Data Security - IT Security

The Company shall ensure that the following measures are taken with respect to IT and information security:

a) All passwords used to protect personal information should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols.;

b) Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Company, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;

c) All software (including, but not limited to, applications and operating systems) shall be kept up to date. The Company's IT staff shall be responsible for installing any and all security-related updates as soon as reasonably and practically possible, unless there are valid technical reasons not to do so;

d) No software may be installed on any Company-owned computer or device without the prior approval of the Information Officer

29. Organisational Measures

The Company shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal information:

a) All employees, agents, contractors, or other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the Protection of Personal Information Act and this Policy, and shall be provided with a copy of this Policy;
b) Only employees, agents, contractors, or other parties working on behalf of the Company that need access to, and use of, personal information in order to carry out their assigned duties correctly shall have access to personal information held by the Company;
c) All sharing of personal information shall comply with the information provided to the relevant data subjects and, if required, the consent of such data subjects shall be obtained prior to the sharing of their personal information;
d) All employees, agents, contractors, or other parties working on behalf of the Company handling personal information will be appropriately supervised;
e) All employees, agents, contractors, or other parties working on behalf of the Company handling personal information shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal information, whether in the workplace or otherwise;
f) Methods of collecting, holding, and processing personal information shall be regularly evaluated and reviewed;
g) All personal information held by the Company shall be reviewed periodically, as set out in the Company's Personal Information Retention Policy;
h) The performance of those employees, agents, contractors, or other parties working on behalf of the Company handling personal information shall be regularly evaluated and reviewed;
i) All employees, agents, contractors, or other parties working on behalf of the Company handling personal information will be bound to do so in accordance with the principles of POPIA and this Policy by contract;
j) All agents, contractors, or other parties working on behalf of the Company handling personal information must ensure that any and all of their employees who are involved in the processing of personal information are held to the same conditions as those relevant employees of the Company arising out of this Policy and POPIA;
k) Where any agent, contractor or other party working on behalf of the Company handling personal information fails in their obligations under this Policy that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure;

30. Transferring Personal information to a Country Outside South Africa

30.1. The Company may, from time to time, transfer ('transfer' includes making available remotely) personal information to countries outside of South Africa. POPIA restricts such transfers to ensure that the level of protection given to data subjects is not compromised.

30.2. Personal information may only be transferred to a country outside the South Africa if one of the following applies:

a) The personal information transferred to another country is protected by appropriate legislation; or
b) adequate safeguards are in place including binding corporate rules; or
c) a binding agreement is concluded between the Company and a third party that offers adequate protection ;or
d) the transfer is made with the informed and explicit consent of the relevant data subject(s); or

e) The transfer is necessary for the performance of a contract between the data subject and the Company; or
f) for the establishment, exercise, or defence of legal claims; or
g) for the benefit of the data subject where it not reasonably practicable to obtain consent from the data subject and the data subject would most likely not have objected;
h) or the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the responsible party and a third party.

30.3. The Company may transfer personal information to:
a) Australia where such information is protected under the Privacy Act of 1988;
b) The United States of America, or any other countries as applicable; and in accordance with an agreement that offers an adequate level of protection;
c) Third parties situated in the European Union where such information is protected under the General Data Protection Regulation (GDPR);
d) The United Kingdom where such information is protected under the UK Data Protection Act of 2018;
e) Countries where the Company's data is stored by online providers such as Google, Microsoft, etc., and in accordance with an agreement that offers an adequate level of protection.

31. Data Breach Notification

31.1. All personal information breaches must be reported immediately to the Company's Information Officer.

31.2. If an employee, agent, contractor, or other party working on behalf of the Company becomes aware of or suspects that a personal information breach has occurred, they must not attempt to investigate it themselves. Any and all evidence relating to the personal information breach in question should be carefully retained.

31.3. If a personal information breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Information Officer must ensure that the Information Regulator's Office as well as the data subject(s) are in writing informed of the breach without delay after having become aware of it, unless such disclosure will interfere with a criminal investigation.

31.4. Data breach notifications shall include the following information:
a) The categories and approximate number of data subjects concerned;
b) The categories and approximate number of personal information records concerned;
c) The name and contact details of the Company's Information Officer (or other contact point where more information can be obtained);
d) The likely consequences of the breach;
e) Details of the measures taken, or proposed to be taken, by the Company to address the breach including, where appropriate, measures to mitigate its possible adverse effects and to prevent it from reoccurring.

32. Employee Personal Information

32.1. The Company holds a range of personal information about its employees. Employee personal information shall be collected, held, and processed in accordance with employee data subjects' rights and the Company's obligations under the Protection of Personal Information Act and with this Policy.

32.2. The Company may collect, hold, and process the employee personal information detailed in this Policy, but not limited to:

Identification and other information relating to employees:

- Name and surname;
- Contact Details;
- Addresses;
- Identification documentation;
- Work permits;
- Bank details;
- Next of kin information;
- Vehicle details (if applicable);
- Fingerprint / retinal images or voice samples for the purposes of access to the workplace and use of company equipment;

Employment Equity monitoring information (Please refer to Part 33, below, for further information):

- Age;
- Gender;
- Ethnicity;
- Nationality;
- Culture;
- Disability;
- Remuneration;

Health records (Please refer to Part 34, below, for further information):

- Details of sick leave;
- Medical conditions;
- Disabilities;
- Medical fitness reports;

Employment records:

- Interview notes;
- CVs, application forms, covering letters, and similar documents;
- Assessments, performance reviews, and similar documents;
- Details of remuneration including salaries, pay increases, bonuses, commission, overtime, benefits, and expenses;
- Details of trade union membership where applicable. Please refer to Part 36, below, for further information);
- Employee monitoring information (please refer to Part 37, below, for further information);
- Records of disciplinary matters including reports and warnings, both formal and informal;
- Details of grievances including documentary evidence, notes from interviews, procedures followed, and outcomes;

33. Employment Equity and Broad Based Black Economic Empowerment Information

33.1. The Company collects, holds, and processes certain information for the purposes of Employment Equity and Broad Based Black Economic Empowerment. Some of the personal information collected for this purpose, such as details of race, gender and disabilities falls within POPIA's definition of special personal information (see Part 2 of this Policy for a definition). Where possible, such special personal information will be de-identified. Where special personal information remains, it will be collected, held, and processed strictly in accordance with the conditions for processing special personal information, as set out in Part 6.2 of this Policy. The Company's lawful basis for processing such data is found in the Employment Equity Act, the Broad Based Black Economic Empowerment Act and relevant regulations.

33.2. Non-anonymised special personal information under this part, shall be accessible and used only by senior management and shall not be revealed to other employees, agents, contractors, or other parties working on behalf of the Company, except in exceptional circumstances where it is necessary to protect the legitimate interests of the employee data subject(s) concerned, and such circumstances satisfy one or more of the conditions set out in Part 6.2 of this Policy.

34. Employee Health Records

34.1. The Company holds health records on employee data subjects which are used to assess the health, wellbeing, and welfare of employees and to highlight any issues which may require further investigation. In particular, the Company places a high priority on maintaining health and safety in the workplace and on preventing discrimination on the grounds of disability or other medical conditions. In most cases, health information on employees falls within POPIA's definition of special personal information (see Part 2 of this Policy for a definition). Any and all data relating to employee data subjects' health, therefore, will be collected, held, and processed strictly in accordance with the conditions for processing special category personal information, as set out in Part 6.2 of this Policy. The Company's lawful basis for processing employees' health information is as provided for in relevant labour related legislation such as The Basic Conditions of Employment Act, The Mines Health and Safety Act, The Occupational Health and Safety Act, the Labour Relations Act and the National Road Traffic Act.

34.2. Health records shall be accessible and used only by Authorised personnel and shall not be revealed to other employees, agents, contractors, or other parties working on behalf of the Company without the express consent of the employee data subject(s) to whom such data relates, except in exceptional circumstances where it is necessary to protect the legitimate interests of the employee data subject(s) concerned, and such circumstances satisfy one or more of the conditions set out in Part 6.2 of this Policy.

34.3. Health records will only be collected, held, and processed to the extent required to justify an employee's absence from work on account of illness and to ensure that employees are able to perform their work correctly, legally, safely, and without unlawful or unfair impediments or discrimination.

35. Employee Benefits

35.1. In cases where employee data subjects are enrolled in benefit schemes which are provided by the Company, it may be necessary from time to time for third party organisations to collect personal information from relevant employee data subjects.

35.2. Prior to the collection of such information, employee data subjects will be fully informed of the personal information that is to be collected, the reasons for its collection, and the manner in which it will be processed, as per the information requirements set out in Part 15 of this Policy.

35.3. The Company shall not use any such personal information except insofar as is necessary in the administration of the relevant benefits schemes.

36. Employee Trade Union Membership

The Company will provide the following personal information concerning relevant employee data subjects to trade unions registered by the Registrar of Labour Relations (Department of Employment and Labour) and where those unions are recognised by the Company. In most cases, information about an individual's trade union membership falls within POPIA's definition of special personal information (see Part 2 of this Policy for a definition). Any and all data relating to employee data subjects' trade union membership, therefore, will be collected, held, and processed strictly in accordance with the conditions for processing special personal information, as set out in Part 6.2 of this Policy. The

Company's lawful basis for processing special personal information relating to trade unions is found in the Labour Relations Act. The following data will be collected and supplied:

a) Name and surname;
b) Employee number;
c) Trade union membership dues;

37. Employee Monitoring

37.1. The Company may from time to time monitor the activities of employee data subjects. Such monitoring may include, but will not necessarily be limited to, internet, email and telephonic communication monitoring, vehicle and electronic communication devices' location tracking, CCTV monitoring of company property, including drivers operating company vehicles and access control to the workplace and/or for the use of Company equipment. In the event that monitoring of any kind is to take place (unless exceptional circumstances, such as the investigation of criminal activity or a matter of equal severity, justify covert monitoring), employee data subjects will be informed of the exact nature of the monitoring in advance.

37.2. Monitoring should not (unless exceptional circumstances justify it, as above) interfere with an employee's normal duties.

37.3. Monitoring will only take place if the Company considers that it is necessary to achieve the benefit it is intended to achieve. Personal information collected during any such monitoring will only be collected, held, and processed for reasons directly related to (and necessary for) achieving the intended result and, at all times, in accordance with employee data subjects' rights and the Company's obligations under the Protection of Personal Information Act.

37.4. The Company shall ensure that there is no unnecessary intrusion upon employee data subjects' personal communications or activities, and under no circumstances will monitoring take place outside of an employee data subject's normal place of work or work hours, unless the employee data subject in question is using any Company equipment or other facilities including, but not limited to, Company email, the Company intranet, a virtual private network ("VPN") service provided by the Company for employee use, Company vehicles or electronic communication, storage and computing devices.

38. Sharing Personal Information of Employee Data Subjects

38.1. The Company will endeavour to only share employee personal information with third parties that have specific safeguards are in place such a POPIA compliance policies.

38.2. Employee personal information may be shared with clients of the Company, other employees, agents, contractors, or other parties working on behalf of the Company if the recipient has a legitimate, job-related need-to-know. If any employee personal information is to be shared with a third party located outside of South Africa, the provisions of Part 30, above, shall also apply.

38.3. Where a third-party Operator is used, that Operator shall process personal information on behalf of the Company only on the written agreement of the Company an in accordance with the guidelines and security measures agreed to.

39. Implementation of Policy

This Policy shall be deemed effective as of 1 July 2021. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

40. Disciplinary Measures

Contravention of this policy, whether intentionally or not, may result in disciplinary action taken. Such disciplinary action may include corrective measures but does not exclude the possibility of termination of employment under certain circumstances.

PERSONAL INFORMATION RETENTION POLICY

1. Introduction

This Policy sets out the obligations of the Company regarding retention of personal information collected, held, and processed by the Company in accordance with the Protection of Personal Information Act. "Protection of Personal Information Act" means all legislation and regulations in force from time to time regulating the protection of personal information, including relevant regulations.

The Protection of Personal Information Act defines "personal information" as any information relating to an identifiable living natural person or existing juristic person (a "data subject"). A data subject can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

The Protection of Personal Information Act also addresses "special personal information". Such information includes, but is not necessarily limited to, information concerning the data subject's race, ethnicity, politics, religion, trade union membership, biometrics, health, sex life or information relating to the criminal behaviour of the data subject in so far as it relates to the alleged commission of an offense.

Under the Protection of Personal Information Act , personal information shall be kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal information is processed.

In addition, the Protection of Personal Information Act includes the right to erasure or "the right to be forgotten". Data subjects have the right to have their personal information erased (and to prevent the processing of that personal information) in the following circumstances:

a) Where the personal information is no longer required for the purpose for which it was
b) originally collected or processed;
c) When the data subject withdraws their consent;
d) When the data subject objects to the processing of their personal information and the Company has no overriding legitimate interest;
e) When the personal information is processed unlawfully (i.e., in breach of the Protection of
f) Personal Information Act); or
g) When the personal information has to be erased to comply with a legal obligation.
h) This Policy sets out the type(s) of personal information held by the Company for specific operational reasons, the period(s) for which that personal information is to be retained, the criteria for establishing and reviewing such period(s), and when and how it is to be deleted or otherwise disposed of.

For further information on other aspects of the protection of personal information and compliance with the Protection of Personal Information Act , please refer to the Company's Protection of Personal Information Policy.

2. Aims and Objectives

The primary aim of this Policy is to set out limits for the retention of personal information and to ensure that those limits, as well as further data subject rights to erasure, are complied with. By extension, this Policy aims to ensure that the Company complies fully with its obligations and the rights of data subjects under the Protection of Personal Information Act.

In addition to safeguarding the rights of data subjects under the Protection of Personal Information Act , by ensuring that excessive amounts of information are not retained by the Company, this Policy also aims to improve the speed and efficiency of managing personal information.

3. Scope

This Policy applies to all personal information held by the Company for operational purposes and where applicable, third party operators processing personal information on the Company's behalf.

Personal information, as held by the Company or its appointed third-party operators is stored in one- or some of the following ways and in the following locations:

a) The Company's appointed Cloud Storage Service Providers with such facilities located;
b) Third-party operators' servers and Cloud Storage facilities;
c) Computers permanently located in the Company's premises;
d) Laptop computers and other mobile devices provided by the Company to its employees;
e) Computers and mobile devices owned by employees, agents, and sub-contractors used in accordance with relevant Company policy;
f) Physical records stored on the premises;
g) Or any other storage types and locations as may be required from time to time

4. Data Subject Rights and Integrity of Personal Information

4.1. All personal information held by the Company is held in accordance with the requirements of the Protection of Personal Information Act and data subjects' rights thereunder, as set out in the Company's Protection of Personal Information Policy.

4.1. Data subjects have the right to be informed of their rights, of what personal information the Company holds about them, how that personal information is used and how long the Company will hold that personal information (or, if no fixed retention period can be determined, the criteria by which the retention of the personal information will be determined).

4.2. Data subjects are given control over their personal information held by the Company including the right to have incorrect information rectified, the right to request that their personal information be deleted or otherwise disposed of (notwithstanding the retention periods otherwise set by this Personal Information Retention Policy, the right to restrict the Company's use of their personal information, and further rights relating to automated decision-making and profiling.

5. Technical and Organisational Data Security Measures

5.1. The following technical measures are in place within the Company to protect the security of personal information. Please refer to the Company's Protection of Personal Information Policy for further details:

a) All emails containing personal information must be encrypted;
b) All emails containing personal information must be marked "confidential";
c) Personal information may not be transmitted over public Wi-Fi networks;
d) Personal information may not be transmitted over a wireless network if there is a reasonable wired alternative;
e) Personal information contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself and associated temporary files should be deleted;
f) Where personal information is to be sent by facsimile transmission the recipient should

be informed in advance and should be waiting to receive it;

g) Where personal information is to be transferred in hardcopy form, it should be passed directly to the recipient or sent using authorised delivery services;
h) All personal information transferred physically should be transferred in a suitable container marked “confidential”;
i) No personal information may be shared informally and if access is required to any personal information, permission must first be granted by the manager responsible for such personal information.
j) All hardcopies of personal information, along with any electronic copies stored on physical media should be stored securely;
k) No personal information may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, without authorisation;
l) Personal information must be handled with care at all times and should not be left unattended or on view;
m) Computers used to view personal information must always be locked before being left unattended;
n) No personal information should be stored on any mobile device, whether such device belongs to the Company or otherwise without the formal written approval of the Information Officer and then strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary;
o) No personal information should be transferred to any device personally belonging to an employee and personal information may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the Company’s Protection of Personal Information Policy, the Protection of Personal Information Act and relevant Company policy pertaining to computer device not owned by the Company;
p) All personal information stored electronically should be backed up frequently with backups stored onsite and/or offsite as specified. All backups should be encrypted;
q) All electronic copies of personal information should be stored securely using passwords and encryption;
r) All passwords used to protect personal information should be changed regularly and must be secure;
s) Under no circumstances should any passwords be written down or shared. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;
t) All software (including, but not limited to, applications and operating systems) shall be kept up to date. The Company’s IT staff shall be responsible for installing any and all security-related updates as soon as reasonably and practically possible, unless there are valid technical reasons not to do so;
u) No software may be installed on any Company-owned computer or device without approval; and
v) Where personal information held by the Company is used for marketing purposes, it shall be the responsibility of the Information Officer to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service.

5.2. The following organisational measures are in place within the Company to protect the security of personal information. Please refer to the Company’s Protection of Personal Information Policy for further details:

a) All employees and other parties working on behalf of the Company shall be made fully

aware of both their individual responsibilities and the Company's responsibilities under the Protection of Personal Information Act and under the Company's Protection of Personal Information Policy;

b) Only employees and other parties working on behalf of the Company that need access to, and use of, personal information in order to perform their work shall have access to personal information held by the Company;
c) All employees and other parties working on behalf of the Company handling personal information will be appropriately trained to do so;
d) All employees and other parties working on behalf of the Company handling personal information will be appropriately supervised;
e) All employees and other parties working on behalf of the Company handling personal information should exercise care and caution when discussing any work relating to personal information at all times;
f) Methods of collecting, holding, and processing personal information shall be regularly evaluated and reviewed;
g) The performance of those employees and other parties working on behalf of the Company handling personal information shall be regularly monitored;
h) All employees and other parties working on behalf of the Company handling personal information will be bound by contract to comply with the Protection of Personal Information Act and the Company's Protection of Personal Information Policy;
i) All agents, contractors, or other parties working on behalf of the Company processing personal information on behalf of the Company must ensure that any and all relevant employees are held to the same conditions as those relevant employees of the Company arising out of the Protection of Personal Information Act and the Company's Protection of Personal Information Policy;
j) Where any agent, contractor or other party working on behalf of the Company handling personal information fails in their obligations under the Protection of Personal Information Act and/or the Company's Protection of Personal Information Policy, that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

6. Disposal of Personal Information

Upon the expiry of the retention periods set out below in Part 7 of this Policy, or when a data subject exercises their right to have their personal information erased, personal information shall be deleted, destroyed, or otherwise disposed of as follows:

a) Special personal information stored electronically (including any and all backups thereof) shall be deleted securely;
b) Personal information stored in hardcopy form shall be shredded to at least 10 mm strips and recycled;
c) Special personal information stored in hardcopy form shall be shredded to at least 6 mm strips and recycled.

7. Retention of Personal Information

7.1. As stated above, and as required by law, the Company shall not retain any personal information for any longer than is necessary in light of the purpose(s) for which that personal information is collected, held, and processed.
7.2. Different types of personal information, used for different purposes, will necessarily be retained for different periods **(**and its retention periodically reviewed), as set out below.
7.3. When establishing and/or reviewing retention periods, the following shall be taken into account:

a) The objectives and requirements of the Company;
b) The type of personal information in question;
c) The purpose(s) for which the personal information in question is collected, held, and processed;
d) The Company's legal basis for collecting, holding, and processing that personal information;
e) The category or categories of data subject to whom the personal information relates;

7.4. If a precise retention period cannot be fixed for a particular type of personal information, criteria shall be established by which the retention of the personal information will be determined, thereby ensuring that the personal information in question, and the retention of that personal information , can be regularly reviewed against those criteria.

7.5. Notwithstanding the following defined retention periods, certain personal information may be deleted or otherwise disposed of prior to the expiry of its defined retention period where a decision is made within the Company to do so (whether in response to a request by a data subject or otherwise).

7.6. In limited circumstances, it may also be necessary to retain personal information for longer periods where such retention is for historical, research or for statistical purposes. All such retention will be subject to the implementation of appropriate technical and organisational measures to protect the rights of data subjects, as required by the Protection of Personal Information Act.

8. Roles and Responsibilities

8.1. The Information Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the Company's other Personal Information Protection-related policies (including, but not limited to, its Protection of Personal Information Policy), and with the Protection of Personal Information Act.

8.2. Any questions regarding this Policy, the retention of personal information, or any other aspect of Protection of Personal Information Act compliance should be referred to the Information Officer.

9. Implementation of Policy

This Policy shall be deemed effective as of 1 July 2021. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

DATA BREACH POLICY

1. Introduction

1.1 This Policy sets out the obligations of the Company regarding the handling and reporting of data breaches and personal information breaches in accordance with the Protection of Personal Information Act ("POPIA").

1.2 The Protection of Personal Information Act defines "personal information" as any information relating to an identifiable living natural person or existing juristic person (a "data subject"). A data subject can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

1.3 For the purposes of this policy, "personal information breach" means the accidental, unlawful or unauthorized access to or acquiring of personal information.

1.4 The Company is under a duty to report personal information breach directly to the Information Regulator's. The Company is also required to inform individual data subjects in the case of breaches.

1.5 All personal information collected, held, and processed by the Company will be handled in accordance with the Company's Personal Information Protection Policy.

1.6 The Company has in place procedures for the detection, investigation, and reporting of data breaches. This Policy applies to all types of data breaches (including personal information breaches) within the Company and is designed to assist in both the handling of such breaches and in determining whether or not they must be reported to the Information Regulator and data subjects.

1.7 The Company's Information Officer and/or appointed Deputy Information Officers, are responsible for the implementation of this Policy, for overseeing the handling of all data breaches, and for ensuring that this Policy is adhered to by all staff.

2. Scope of Policy

2.1. This Policy relates to all formats of data (including personal information and special personal information under POPIA, collected, held, and processed by the Company.

2.2. This Policy applies to all staff of the Company, including but not limited to employees, agents, contractors, consultants, temporary staff, casual or agency staff, or other suppliers or personal information processing operators working for or on behalf of the Company.

2.3. This Policy applies to all data breaches, whether suspected or confirmed.

3. Data Breaches

3.1. For the purposes of this Policy, a data breach means any event or action (accidental or deliberate) which presents a threat to the security, integrity, confidentiality, or availability of data.

3.2. Incidents to which this Policy applies may include, but not be limited to:

a) the loss or theft of a physical data record;
b) the loss or theft of computer equipment (e.g. laptop), mobile devices (e.g. smartphone or tablet), portable data storage devices (e.g. USB drive), or other data storage devices;
c) equipment failure;
d) unauthorised access to, use of, or modification of data (or inadequate access controls allowing unauthorised access, use, or modification);
e) unauthorised disclosure of data;
f) human error (e.g., sending data to the wrong recipient);
g) unforeseen circumstances such as fire or flood;

h) hacking, phishing, and other 'blagging" (tracing) offences whereby information is obtained by deception;

4. Internal Reporting

4.1. If a data breach is discovered or suspected, members of staff should complete a Data Breach Report Form, and send the completed form to the Company's Information Office and/or appointed Deputy Information Officers.

4.2. A completed Data Breach Report Form should include full and accurate details about the incident including, but not limited to (where applicable):

a) the time and date of the breach;
b) the time and date the breach was discovered;
c) the type(s) of data involved;
d) where the breach involves personal information, the categories(s) of data subject to which the personal information relates (e.g. customers, employees etc.);
e) whether or not any special personal information is involved;
f) how many data subjects are likely to be affected (if known);

4.3. Where appropriate, members of staff should liaise with their Line Manager when completing a Data Breach Report Form.

4.4. If a data breach occurs or is discovered outside of normal working hours, it should be reported as soon as is reasonably practicable.

4.5. Unless and until instructed to by the Company's Information Officer and/or appointed Deputy Information Officers, members of staff should not take any further action with respect to a data breach. In particular, individual members of staff should not take it upon themselves to notify affected data subjects, the Information Regulator, or any other individuals or organisations.

5. Initial Management and Recording

5.1. Upon receipt of a Data Breach Report Form (or upon being notified of a data breach in any other way), the Company's Information Officer and/or appointed Deputy Information Officers shall begin by determining whether the data breach is still occurring. If this is the case, appropriate steps shall be taken immediately to minimise the effects of the data breach and to stop it.

5.2. Having established the above, the following steps shall then be taken with respect to the data breach:

a) undertake an initial assessment of the data breach, liaising with the relevant staff and departments where appropriate, to establish the severity of the data breach;
b) contain the data breach and, to the extent reasonably practicable, recover, amend, or restrict the availability of (e.g. by changing or revoking access permissions or by temporarily making the data unavailable electronically) the affected data;
c) determine whether anything further can be done to recover the data and/or other losses, and to limit the damage caused by the breach;
d) establish who needs to be notified initially (including, if physical records or equipment have been lost or stolen, the police) as part of the initial containment;
e) determine, in liaison with the relevant staff and departments, the best course of action to resolve and remedy the data breach; and
f) record the breach and the initial steps taken above in the Company's Data Breach Register.

5.3. Having completed the initial steps described above, the Company's Information Officer and/or appointed Deputy Information Officers shall proceed with investigating and assessing the data breach as described in Part 6, below.

6. Investigation and Assessment

6.1. The Company's Information Officer and/or appointed Deputy Information Officers shall begin an investigation of a data breach as soon as is reasonably possible after receiving a Data Breach Report Form (or being notified in any other way) and, in any event, within 24 hours of the data breach being discovered and/or reported.

6.2. Investigations and assessments must take the following into account:

a) the type(s) of data involved (and, in particular, whether the data is personal information or special personal information);
b) the sensitivity of the data (both commercially and personally);
c) what the data breach involved;
d) what organisational and technical measures were in place to protect the data;
e) what might be done with the data as a result of a breach (including unlawful or otherwise inappropriate misuse);
f) where personal information is involved, what that personal information could tell a third party about the data subjects to whom the data relates;
    i. the category or categories of data subject to whom any personal information relates;
    ii. the number of data subjects (or approximate number if calculating an exact number is not reasonably practicable) likely to be affected by the data breach;
    iii. the potential effects on the data subjects involved;
    iv. the potential consequences for the Company;
    v. the broader consequences of the data breach, both for data subjects and for the Company;
    vi. measures that can be taken to prevent similar data breaches.

6.3. The results of the investigation and assessment described above must be recorded in the Company's Data Breach Register.

6.4. Having completed the investigation and assessment described above, the Company's Information Officer and/or appointed Deputy Information Officers shall determine the parties to be notified of the breach as described in Part 7, below.

7. Notification

7.1. The Company's Information Officer shall determine whether to notify one or more of the following parties of the breach:

a) affected data subjects;
b) the Information Regulator;
c) the police;
d) the Company's insurers;
e) affected commercial partners;

7.2. When considering whether and how to notify the Information Regulator and individual data subjects in the event of a personal information breach, it must be considered whether such notification will interfere with a criminal investigation. In this regard guidance is to be sought from a public body responsible for the prevention, detection or investigation of offences, relevant to the data breach. Alternatively, it may be determined by the Information Regulator whether notification will impede a criminal investigation by the public body concerned.

7.3. When individual data subjects are to be informed of a data breach, those individuals must be informed of the breach without undue delay. Individuals shall be provided with the following information:

a) a user-friendly description of the data breach, including how and when it occurred, the personal information involved, and the likely consequences;
b) clear and specific advice, where relevant, on the steps individuals can take to protect themselves;

c) a description of the measures taken (or proposed to be taken) to address the data breach including, where relevant, measures taken to mitigate any possible adverse effects;
d) contact details for the Company's Information Officer and/or appointed Deputy Information Officers from whom affected individuals can obtain further information about the data breach.

7.4. If the Information Regulator is to be notified of a breach of personal information within 72 hours, excluding weekends and public holidays, of becoming aware of the breach, where feasible. This time limit applies even if complete details of the data breach are not yet available. The Information Regulator must be provided with the following information:
a) the category or categories and the approximate number of data subjects whose personal information is affected by the data breach;
b) the category or categories and the approximate number of personal information records involved;
c) the name and contact details of the Company's Information Officer from which the Information Regulator can obtain further information about the data breach;
d) a description of the likely consequences of the data breach; and
e) a description of the measures taken (or proposed to be taken) to address the data breach including, where relevant, measures taken to mitigate any possible adverse effects.

7.5. Records must be kept of all data breaches, regardless of whether notification is required to the Information Regulator. The decision-making process surrounding notification should be documented and recorded in the Company's Data Breach Register.

8. Evaluation and Response

8.1. When the steps set out above have been completed, the data breach has been contained, and all necessary parties notified, the Company's Information Officer and appointed deputies, shall conduct a complete review of the causes of the data breach, the effectiveness of the measures taken in response, and whether any systems, policies, or procedures can be changed to prevent data breaches from occurring in the future.

8.2. Such reviews shall, in particular, consider the following with respect to data (and in particular, personal information) collected, held, and processed by the Company:
a) where and how data is held and stored;
b) the current organisational and technical security measures in place to protect data and the risks and possible weaknesses of those measures;
c) the methods of data transmission for both physical and electronic data and whether or not such methods are secure;
d) the level of data sharing that takes place and whether or not that level is necessary;
e) whether any data protection impact assessments need to be conducted or updated;
f) staff awareness and training concerning data protection;
g) whether disciplinary action is to be instituted against any employee whose actions, whether directly or indirectly, resulted in the data breach.

8.3. Where possible improvements and/or other changes are identified, **[**the Company's Information Officer and/or appointed deputies shall liaise with relevant staff and/or departments with respect to the implementation of such improvements and/or changes.

9. Policy Review and Implementation

9.1. This Policy will be updated as necessary to reflect current best practice, official guidance, and in line with current legislation.

9.2. This Policy shall be deemed effective as of 1 July 2021. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

DATA SECURITY POLICY

1. Introduction

1.1 This document sets out the measures to be taken by all employees of the Company and by the Company as a whole in order to protect data (electronic and otherwise) collected, held, and processed by the Company, and to protect the Company's computer systems, devices, infrastructure, computing environment, and any and all other relevant equipment (collectively, "IT Systems") from damage and threats whether internal, external, deliberate, or accidental.

1.2 This Policy shall be, where applicable, subject to and interpreted in accordance with, the Protection of Personal Information Act ("POPIA").

1.3 For the purposes of this Policy, "personal information" shall carry the meaning defined in POPIA as any information relating to an identified living natural person or existing juristic person (a "data subject"), such as defined in the Company's Protection of Personal Information Policy.

2. Key Principles

2.1. All IT Systems and data are to be protected against unauthorised access.

2.2. All IT Systems and data are to be used only in compliance with relevant Company Policies.

2.3. All personal information must be used only in compliance with POPIA and the Company's Personal Information Protection Policy.

2.4. All employees of the Company and any and all third parties authorised to use the IT Systems and data collected, held, and processed by the Company including, but not limited to, contractors and sub-contractors (collectively, "Users"), must ensure that they are familiar with this Policy and must adhere to and comply with it at all times.

2.5. All line managers must ensure that all Users under their control and direction must adhere to and comply with this Policy at all times as required under paragraph 2.4.

2.6. All data must be managed securely in compliance with relevant legislation, whether now or in the future in force.

2.7. All data must be classified appropriately (including, but not limited to, personal information, special personal information or confidential information). All data so classified must be handled appropriately in accordance with its classification.

2.8. All data, whether stored on IT Systems or in hardcopy format, shall be available only to those Users with a legitimate need for access.

2.9. All data, whether stored on IT Systems or in hardcopy format, shall be protected against unauthorised access and/or processing.

2.10. All data, whether stored on IT Systems or in hardcopy format, shall be protected against loss and/or corruption.

2.11. All IT Systems are to be installed, maintained, serviced, repaired, and upgraded by the "IT Department" or by such third party/parties as the IT Department may from time to time authorise.

2.12. The responsibility for the security and integrity of all IT Systems and the data stored thereon (including, but not limited to, the security, integrity, and confidentiality of that data) lies with the IT Department unless expressly stated otherwise.

2.13. The responsibility for the security and integrity of data that is not stored on the IT Systems lies with the Heads of Departments.

2.14. All breaches of security pertaining to the IT Systems or any data stored thereon shall be reported and subsequently investigated by the IT Department. Any breach which is either known or suspected to involve personal information shall be reported to the Information Officer or any of the appointed Deputy Information Officers.

2.15. All breaches of security pertaining to data that is not stored on the IT Systems shall be reported and subsequently investigated by the Company. Any breach which is either known or suspected

to involve personal information shall be reported to the Information Officer or any of the appointed Deputy Information Officers.

2.16. All Users must report any and all security concerns relating to the IT Systems or to the data stored thereon immediately to the IT Department. If any such concerns relate in any way to personal information, such concerns must also be reported to the Information Officer.

2.17. All Users must report any and all security concerns relating to data that is not stored on the IT Systems immediately to, the Head of the Department. If any such concerns relate in any way to personal information, such concerns must also be reported to the Information Officer or any of the appointed Deputy Information Officers.

3. Department Responsibilities

3.1. The IT Manager shall be responsible for the following:

a) ensuring that all IT Systems are assessed and deemed suitable for compliance with the Company's security requirements;

b) ensuring that IT security standards within the Company are effectively implemented and regularly reviewed, working in consultation with the Company's senior management and Information Officer, as appropriate, and reporting the outcome of such reviews to the Company's senior management and the Information Officer;

c) ensuring that all Users are kept aware of the IT-related requirements of this Policy and of all related legislation, regulations, and other relevant rules whether now or in the future in force including, but not limited to, the Protection of Personal Information Act no. 4 of 2013.

3.2. The appointed Deputy Information Officers shall be responsible for the following:

a) ensuring that all other data processing systems and methods are assessed and deemed suitable for compliance with the Company's security requirements;

b) ensuring that data security standards within the Company are effectively implemented and regularly reviewed, working in consultation with the Company's senior management and Information Officer, as appropriate, and reporting the outcome of such reviews to the Company's senior management and the Information Officer;

c) ensuring that all Users are kept aware of the non-IT-related requirements of this Policy and of all related legislation, regulations, and other relevant rules whether now or in the future in force including, but not limited to, the Protection of Personal Information Act No. 4 of 2013.

3.3. The IT Staff shall be responsible for the following:

a) assisting all Users in understanding and complying with the IT-related aspects of this Policy;

b) providing all Users with appropriate support and training in IT security matters and use of IT Systems;

c) ensuring that all Users are granted levels of access to IT Systems that are appropriate for each User, taking into account their job role, responsibilities, and any special security requirements;

d) receiving and handling all reports relating to IT security matters and taking appropriate action in response including, in the event that any reports relate to personal information, informing the Information Officer;

e) taking proactive action, where possible, to establish and implement IT security procedures and raise User awareness;

f) assisting the IT Manager in monitoring all IT security within the Company and taking all necessary action to implement this Policy and any changes made to this Policy in the future; and

g) ensuring that regular backups are taken of all data stored within the IT Systems at intervals no less than 12 months and that such backups are stored at a suitable location. All backups should be encrypted.

3.4. The Heads of Departments shall be responsible for the following:

a) assisting all Users in understanding and complying with the non-IT-related aspects of this Policy;

b) providing all Users with appropriate support and training in data security matters;

c) ensuring that all Users are granted levels of access to data that are appropriate for each User, taking into account their job role, responsibilities, and any special security requirements;

d) receiving and handling reports concerning non-IT-related data security matters and taking appropriate action in response including, in the event that any reports relate to personal information, informing the Information Officer or any of the appointed Deputy Information Officers;

e) taking proactive action, where possible, to establish and implement security procedures and raise User awareness; and

f) assisting the Information Officer and appointed Deputy Information Officers in monitoring data security within the Company and taking all necessary action to implement this Policy and any changes made to this Policy in the future.

4. Users' Responsibilities

4.1. All Users must comply with all relevant parts of this Policy at all times when using the IT Systems and data.

4.2. All Users must use the IT Systems and data only within the bounds of South African legislation and must not use the IT Systems or data for any purpose or activity which is likely to contravene any legislation or Company policy whether now or in the future in force.

4.3. Users must immediately inform the IT Department and/or Head of the Department and, where such concerns relate to personal information, the Information Officer or any of the appointed Deputy Information Officers of any and all security concerns relating to the IT Systems or data.

4.4. Users must immediately inform the IT Department of any other technical problems (including, but not limited to, hardware failures and software errors) which may occur on the IT Systems.

4.5. Any and all deliberate or negligent breaches of this Policy by Users will be handled as appropriate under the Company's disciplinary procedures.

5. Software Security Measures

5.1. All software in use on the IT Systems (including, but not limited to, operating systems, individual software applications, and firmware) will be kept up-to-date and any and all relevant software updates, patches, fixes, and other intermediate releases will be applied at the sole discretion of the IT Department. This provision does not extend to upgrading software to new 'major releases' (e.g., from version 1.0 to version 2.0), only to updates within a particular major release (e.g., from version 1.0 to version 1.0.1 etc.). Unless a software update is available free of charge it will be classed as a major release, falling within the remit of new software procurement and outside the scope of this provision.

5.2. Where any security flaw is identified in any software that flaw will be either fixed immediately or the software may be withdrawn from the IT Systems until such time as the security flaw can be effectively remedied.

5.3. No Users may install any software of their own, whether that software is supplied on physical media or whether it is downloaded, without the approval of the IT Manager. Any software belonging to Users must be approved by the IT Manager and may only be installed where that installation poses no security risk to the IT Systems and where the installation would not breach

any licence agreements to which that software may be subject.

5.4. All software will be installed onto the IT Systems by the IT Department unless an individual User is given written permission to do so by the IT Manager. Such written permission must clearly state which software may be installed and onto which computer(s) or device(s) it may be installed.

6. Anti-Virus Security Measures

6.1. Most IT Systems (including all computers and servers) will be protected with suitable anti-virus, firewall, and other suitable internet security software. All such software will be kept up to date with the latest software updates and definitions.

6.2. All IT Systems protected by anti-virus software will be subject to a full system scan at least quarterly.

6.3. All physical media (e.g., USB memory sticks or disks of any kind) used by Users for transferring files must be virus-scanned before any files may be transferred.

6.4. Any files being sent to third parties outside the Company, whether by email, on physical media, or by other means (e.g., shared cloud storage) must be scanned for viruses before being sent or as part of the sending process, as appropriate.

6.5. Where any virus is detected by a User this must be reported immediately to the IT Department (this rule shall apply even where the anti-virus software automatically fixes the problem). The IT Department shall promptly take any and all necessary action to remedy the problem. In limited circumstances this may involve the temporary removal of the affected computer or device.

6.6. If any virus or other malware affects, is likely to affect, or is suspected to affect any personal information, in addition to the above, the issue must be reported immediately to the Information Officer or any of the appointed Deputy Information Officers.

6.7. Where any User deliberately introduces any malicious software or virus to the IT Systems this will constitute a dismissible offence under the Company's disciplinary procedures.

7. Hardware Security Measures

7.1. Wherever practical, IT Systems will be located in rooms which may be securely locked when not in use or, in appropriate cases, at all times whether in use or not (with authorised Users being granted access by means of a key, smart card, door code or similar). Where access to such locations is restricted, Users must not allow any unauthorised access to such locations for any reason.

7.2. All IT Systems not intended for normal use by Users (including, but not limited to, servers, networking equipment, and network infrastructure) shall be located, wherever possible and practical, in secured, climate-controlled rooms and/or in locked cabinets which may be accessed only by designated members of the IT Department.

7.3. No Users shall have access to any IT Systems not intended for normal use by Users (including such devices mentioned above) without the express permission of the IT Manager. Under normal circumstances, whenever a problem with such IT Systems is identified by a User, that problem must be reported to the IT Department. Under no circumstances should a User attempt to rectify any such problems without the express permission (and, in most cases, instruction and/or supervision) of the IT Manager.

7.4. All non-mobile devices (including, but not limited to, desktop computers, workstations, and monitors) shall, wherever possible and practical, be physically secured in place with a suitable locking mechanism. Where the design of the hardware allows, computer cases shall be locked to prevent tampering with or theft of internal components.

7.5. All mobile devices (including, but not limited to, laptops, tablets, and smartphones) provided by the Company should always be transported securely and handled with care. In circumstances

where such mobile devices are to be left unattended they should be placed inside a lockable case or other suitable container. Users should make all reasonable efforts to avoid such mobile devices from being left unattended at any location other than their private homes or Company premises.

7.6. The IT Department shall maintain a complete asset register of all IT Systems. All IT Systems shall be labelled, and the corresponding data shall be kept on the asset register.

8. Organisational Security

8.1. All Users handling data (and in particular personal information) will be appropriately trained to do so.

8.2. All Users handling data (and in particular personal information) will be appropriately supervised.

8.3. All Users handling data (and in particular personal information) shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to such data, whether in the workplace or otherwise.

8.4. Methods of collecting, holding, and processing data (and in particular personal information) shall be regularly evaluated and reviewed.

8.5. All personal information held by the Company shall be reviewed periodically, as set out in the Company's Personal Information Retention Policy.

8.6. All Users handling personal information will be bound to do so in accordance with the principles of the Protection of Personal Information Act no. 4 of 2013 and relevant Company policies.

8.7. No data, personal or otherwise, may be shared informally and if a User requires access to any data, personal or otherwise, that they do not already have access to, such access should be formally requested from the Head of the Department.

8.8. No data, personal or otherwise, may be transferred to any unauthorised User without the authorisation of the Head of the Department.

8.9. All data must be handled with care at all times and should not be left unattended or on view to unauthorised Users or other parties at any time.

9. Access Security

9.1. Access privileges for all IT Systems and data shall be determined on the basis of Users' levels of authority within the Company and the requirements of their job roles. Users shall not be granted access to any IT Systems or data which are not reasonably required for the fulfilment of their job roles.

9.2. All IT Systems (and in particular mobile devices including, but not limited to, laptops, tablets, and smartphones) shall be protected with a secure password or passcode, or such other form of secure log-in system as the IT Department may deem appropriate and approve. Not all forms of biometric log-in are considered secure. Only those methods approved by the IT Department may be used.

9.3. Passwords should be kept secret by each User. Under no circumstances should a User share their password with anyone, including the IT Manager and the IT Staff. No User will be legitimately asked for their password by anyone at any time and any such request should be refused. If a User has reason to believe that another individual has obtained their password, they should change their password immediately and report the suspected breach of security to the IT Department and, where personal information could be accessed by an unauthorised individual, the Information Officer or any of the appointed Deputy Information Officers.

9.4. If a User forgets their password, this should be reported to the IT Department. The IT Department will take the necessary steps to restore the User's access to the IT Systems which may include the issuing of a temporary password which may be fully or partially known to the member of the IT Staff responsible for resolving the issue. A new password must be set up by the User immediately upon the restoration of access to the IT Systems.

9.5. Users should not write down passwords if it is possible to remember them. If a User cannot remember a password, it should be stored securely (e.g., in a locked drawer or in a secure password database) and under no circumstances should passwords be left on display for others to see (e.g., by attaching a note to a computer display).

9.6. All IT Systems with displays and user input devices (e.g., mouse, keyboard, touchscreen etc.) shall be protected, where possible, with a password protected screensaver that will activate after a set time of inactivity. This time period cannot be changed by Users and Users may not disable the screensaver. Activation of the screensaver will not interrupt or disrupt any other activities taking place on the computer (e.g., data processing).

9.7. All mobile devices (including, but not limited to, laptops, tablets, and smartphones) provided by the Company shall be set to lock, sleep, or similar, after a set period of inactivity, requiring a password, passcode, or other form of log-in to unlock, wake, or similar. Users may not alter this time period.

9.8. Users may not use any software which may allow outside parties to access the IT Systems without the express consent of the IT Manager. Any such software must be reasonably required by the User for the performance of their job role and must be fully inspected and cleared by the IT Manager and, where such access renders personal information accessible by the outside party, the Information Officer or any of the appointed Deputy Information Officers.

10. Data Storage Security

10.1 All data stored in electronic form, and in particular personal information, should be stored securely using passwords and data encryption.

10.2 All data stored in hardcopy format or electronically on removable physical media, and in particular personal information, should be stored securely in a locked box, drawer, cabinet, or similar.

10.3 No data, and in particular personal information, should be transferred to any computer or device personally belonging to a User unless the User in question is a contractor or sub-contractor working on behalf of the Company and that User has agreed to comply fully with the Company's Protection of Personal Information Policy and the Protection of Personal Information Act no. 4 of 2013.

10.4 No data, and in particular personal information, should be transferred to any computer or device personally belonging to a User that is an employee, unless written permission has been granted and subject to the requirements pertaining to Data Security as set out in this policy as well as the Company's Protection of Personal Information Policy.

11. Protection of Personal Information

11.1. All personal information collected, held, and processed by the Company will be collected, held, and processed strictly in accordance with the principles of the Protection of Personal Information Act no. 4 of 2013 and the Company's Protection of Personal Information Policy.

11.2. All Users handling personal information for and on behalf of the Company shall be subject to, and must comply with, the provisions of the Company's Protection of Personal Information Policy at all times. In particular, the following shall apply:

a) All emails containing personal information must be encrypted
b) Personal information may be transmitted over secure networks only; transmission over unsecured networks is not permitted under any circumstances;
c) Personal information may not be transmitted over public wireless networks;
d) All personal information to be transferred physically, including that on removable electronic media, shall be transferred in a suitable container marked "confidential".

e) Where any personal information and/or other data covered by this Policy is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the User must lock the computer and screen before leaving it.

12. Deletion and Disposal of Data

12.1. When any data, and in particular personal information, is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it must be securely deleted and/or disposed of.

12.2. For further information on the deletion and disposal of personal information, please refer to the Company's Personal Information Retention Policy.

13. Internet and Email Use

13.1. All Users shall be subject to, and must comply with, the provisions of relevant Company policies pertaining to Communications, Email and Internet when using the IT Systems.

13.2. Where provisions in this Policy require any additional steps to be taken to ensure security when using the internet or email over and above the requirements imposed by other policies, Users must take such steps as required.

14. Reporting Security Breaches

All security breaches, whether relating to personal information or not, shall be dealt with in accordance with the Company's Data Breach Policy.

15. Policy Review

The Company shall, if so required, review this Policy every 18 months and otherwise as required in order to ensure that it remains up-to-date and fit for purpose.

16. Implementation of Policy

This Policy shall be deemed effective as of 1 July 2021. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

DATA SUBJECT ACCESS REQUEST POLICY

2. Introduction

This Policy sets out the obligations of the Company regarding data subject access requests under the Protection of Personal Information Act no. 4 of 2013.

This Policy also provides guidance on the handling of data subject access requests. The procedures and principles set out herein must be followed at all times by the Company, its employees, agents, contractors, or other parties working on behalf of the Company.

3. Definitions

"responsible party"	means the natural or legal person or organisation which, alone or jointly with others, determines the purposes and means of the processing of personal information. For the purposes of this Policy, the Company is the responsible party for all personal information relating to data subjects such as employees, customers, business contacts, etc. used in our business for our commercial purposes;
"operator"	means a natural or legal person or organisation which processes personal information on behalf of a responsible party;
"data subject"	means a living identifiable natural person or existing juristic person about whom the Company holds personal information;
"personal information"	Means any information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to— (a) information relating to the race, gender, sex, pregnancy, marital status, nationality, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person; (b) information relating to the education or the medical, financial, criminal or employment history of the person; (c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person; (d) the biometric information of the person; (e) the personal opinions, views or preferences of the person; (f) 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; (g) the views or opinions of another individual about the person; and (h) 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;
"processing"	means any operation or set of operations performed on personal information or sets of personal information, whether or not by automated means, such as but not limited to the collection, receipt, recording, organisation, structuring, storage, adaptation / alteration, retrieval, use, disclosure by transmission/dissemination or otherwise making available, alignment, merging, linking/combining, restriction, erasure or destruction thereof.

"special personal information"	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 (b) the criminal behaviour of a data subject to the extent that such information relates to— (i) the alleged commission by a data subject of any offence; or (ii) any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

3. Information Officer & Scope of Policy

3.1. The Information Officer is responsible for administering this Policy; for developing and implementing any applicable related policies (including those referred to in this Policy), procedures, and/or guidelines; for ensuring that all data subject access requests are handled in accordance with the Protection of Personal Information Act and the Promotion of Access to Information Act; and for ensuring that all employees, agents, contractors, or other parties working on behalf of the Company have an understanding of the Protection of Personal Information Act and their obligations under it as it applies to their job role(s).

3.2. The Company collects, holds, and processes personal information of its employees, customers, business contacts, etc. The Company is a 'responsible party' for the purposes of the Protection of Personal Information Act.

3.3. Data subjects have rights with respect to their personal information under the Protection of Personal Information Act. This Policy deals specifically with the right of access (sections 5, 23 and 24 of the Protection of Personal Information Act). Data subjects have the right to find out whether the Company collects, holds, or processes personal information about them, the right to obtain a copy of any such information, and certain other supplementary information. The right of access is designed to help data subjects to understand how and why we use their information, and to check that we are doing so lawfully.

3.4. This Policy is an internal company policy designed to provide guidance on handling data subject access requests. It is not a personal information protection policy, privacy policy, privacy notice, or similar, and is not designed to be made available to third parties (including, but not limited to, data subjects). This Policy should, where appropriate, be read in conjunction with the Company's Personal Information Protection Policy and Privacy Notice.

3.5. Any questions relating to this Policy, the Company's collection, processing, or holding of personal information, or to the Protection of Personal Information Act should be referred to the Information Officer.

3.6. Parts 1 to 4 and Parts 14 to 16 of this Policy apply to all staff and Parts 5 to 13 apply to staff authorised to handle data subject access requests.

4. How to Recognise a Data Subject Access Request

4.1. The Protection of Personal Information Act does not set out a particular format which a data subject access request (hereafter "SAR") must follow. A SAR may be made orally or in writing, to any part of the Company, and by any means of communication. This means that anyone in the Company could receive a SAR and it may not be immediately obvious that a SAR has been received.

4.2. The Company provides a Subject Access Request Form, available from the office, to make it easier for data subjects to make a SAR and to make it easier for the Company to recognise the request; however, data subjects may not be aware of the SAR form and care must be taken at all times to identify SARs made in other ways.

4.3. SARs may instead use more general terminology, using terms such as 'information' rather than 'personal information'. For example, a message sent to the Company via social media such as

'please provide details of all the information you have about me'. **Under such circumstances, data subject must be advised to complete the Subject Access Request Form 1 (SAR from 1).**

4.4. When a SAR is identified, or if a communication or request is received and you are in anyway unsure whether or not it is a SAR, it should be immediately forwarded to the Company's Information Officer, or to any one of the appointed Deputy Information Officers.

5. What to do When a Subject Access Request is Received

5.1. The Company must deal with a SAR in an expeditious manner, so it is important to act quickly.

5.2. Unless you are authorised to handle a SAR, it must be forwarded to the Information Officer and / or any of the appointed Deputy Information Officers, as set out in this Part 5. Please do not take any further action with respect to any SAR unless you are authorised to do so.

5.3. SARs made by submitting SAR Form 1 or any other informal method must be immediately forwarded per email to the Company's Information Officer, or to any one of the appointed Deputy Information Officers.

5.4. The Company's Information Officer or appointed Deputy Information Officer should respond to you, confirming receipt of the SAR, within 48 hours of you sending it. If you do not receive a response within this period, you must contact them again to confirm receipt.

6. Responding to a Subject Access Request Part 1: Identifying Data Subjects and Clarifying Requests (only for Information Officer or appointed Deputy Information Officers).

6.1. Before responding to a SAR, all reasonable steps must be taken to verify the identity of the individual making the request and, particularly if the Company is processing a large amount of personal information about them, to clarify their request (i.e., to specify the personal information or processing to which their SAR relates). Information requested for such purposes must be reasonable and proportionate. Individuals must not be asked to provide any more information than is reasonably necessary, nor can a request for clarification be used to narrow the scope of a SAR.

6.2. Upon receipt of SAR Form 1, confirmation of receipt and, if applicable, a request for additional information, must be made using SAR Form 2.

6.3. If a SAR is made by a third party on behalf of a data subject, the individual acting on behalf of the data subject must be required to provide sufficient evidence that they are authorised to act on the data subject's behalf.

6.4. Examples of information that may be requested to confirm an individual's identity include:

a) A copy of the individual's identity document;

b) A copy of the individual's driving licence;

6.5. If, having requested additional information to verify an individual's identity, it is still not possible to do so (if, for example, the individual does not comply), the Company may refuse to comply with a SAR, as set out below in Part 11.

6.6. If, having requested additional information to clarify a SAR, the individual does not comply (e.g., does not respond, or refuses to provide further information), the Company must still endeavour to comply with the SAR by making reasonable searches for the personal information relating to the request.

6.7. Upon receipt of the additional information that may have been requested, SAR Form 3 Must be completed and sent to the data subject.

7. Responding to a Subject Access Request Part 2: Fees

7.1. Under normal circumstances, the Company does not normally charge for a request to only confirm whether the personal information of the data subject is kept by the Company.

7.2. It is permissible to charge a fee to cover the administrative costs of complying with a SAR in so far as it relates to the disclosure of personal information processed by the Company.

7.3. In certain cases, it may also be permissible to refuse to comply with a SAR, as set out in Part 11(b).

7.4. The following factors should be considered when calculating a reasonable fee:

a) Administrative costs involved in:
   i. Assessing whether or not the Company is processing the data subject's information;
   ii. Locating, retrieving, and extracting that information;
   iii. Providing a copy of the information; and
   iv. Sending the Company's response to the data subject.

b) Specific costs to be considered include:
   i. Photocopying, printing, postage, and any other costs incurred when sending the information to the data subject;
   ii. Equipment and supplies; and
   iii. Staff time.

8. Responding to a Subject Access Request Part 3: Time Limits

8.1. Under normal circumstances, the Company must respond to a SAR within one month of receipt. The date of receipt of all SARs must be recorded, along with the due date for response.

8.2. The one-month period referred to in Part 8.1 begins on the calendar day – not business day – that the request is received and ends on the corresponding calendar day in the following month (or, if the following month is shorter and does not have a corresponding day (e.g., January 31st to February 28th), the last day of that month. If the last day of the time limit falls on a weekend or public holiday, the time limit is extended to the next business day.

8.3. If additional information is required from the individual making the SAR to confirm an individual's identity, as under Part 6.2, the time limit under Part 8.1 begins on the day that such information is received.

8.4. If additional information is required from the individual making the SAR to clarify the SAR, as under part 6.3, the time limit under Part 8.1 is paused until the information is received (unless the response is received on the same day, in which case the time limit is not affected).

8.5. If the SAR is complex, or if the same data subject makes a number of SARs, the time limit may be extended up to two months. If such an extension is necessary, the data subject must be informed, in writing using SAR Form 4, of the reason(s) for the extension within the original one-month time limit.

9. Responding to a Subject Access Request Part 4: Information to be Provided and action to be taken

9.1. Data subjects may in example be provided with the following information in response to a SAR:

a) the personal information requested;
b) the purposes for which the Company collects, holds, and processes their personal information;
c) the categories of personal information involved;
d) the recipients or categories of recipient to whom the Company discloses their personal information, including third parties;
e) details of how long the Company retains their personal information or, if there is no fixed period, our criteria for determining how long it will be retained;
f) details of the data subject's right to make a complaint to the Information Regulator;
g) if any of the personal information in question was not obtained from the data subject, details of the source of that data;
h) if the Company carries out any automated decision-making (including profiling), details of that automated decision-making, including a meaningful explanation of the logic involved

and the significance and envisaged consequences for the data subject (also see Part 9.2); and

i) if the Company transfers their personal information to another country, details of the safeguards in place to protect that information.

9.2. In cases where a SAR relates to automated decision-making, the following shall apply:

a) Where a SAR relates to the logic underlying an automated decision that has been taken with respect to important matters relating to the data subject, the data subject must be provided with an explanation of the logic involved, subject to the following conditions:

i. the decision-making process in question must be solely automated (i.e., there must be no human involvement in the process); and

ii. the information should be provided in such a way as to protect the Company's intellectual property rights and trade secrets.

9.3. It is important to note that data subjects are only entitled to access personal information that the Company holds about them. If information located in the process of responding to a SAR does not meet the definition of "personal information" (see Part 1), the Protection of Personal Information Act does not entitle the data subject to access it. If applicable, the data subject may then rely on the Promotion of Access to Information Act to attempt to gain access to such information.

9.4. If a data subject requests the Company to correct or delete personal information about the data subject, the Company may correct, destroy or delete the information if it is inaccurate, misleading, out of date, incomplete, obtained unlawfully, or the Company is no longer authorized to be in possession of the information.

9.5. The Company must notify the data subject, in writing, of the action taken in terms of Part 9.4, as a result of the SAR. 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 has been requested but has not been made.

9.6. If a data subject objects against the processing of personal information on the basis of protecting a legitimate interest of either the data subject, the Company or a third party to whom the personal information is supplied, or for the purposes of direct marketing by means of electronic communication only, the Company may no longer process such personal information. The data subject must accordingly be informed about the consequences thereof, if any.

10. Responding to a Subject Access Request Part 5: Locating Information

10.1. The Company holds personal information at various locations and formats. It is important to identify the type(s) of personal information to which a SAR relates in order to search in the correct place.

10.2. The Company must make a reasonable effort to find and retrieve personal information in response to a SAR. The right of access is not limited to that information which is easy to find.

11. Refusing to Respond to a Subject Access Request

11.1 In certain cases, the Company may refuse to comply with a SAR:

a) if it is not possible to identify the individual making the SAR after requesting additional verification under Part 6.2; or

b) if the request is 'manifestly unfounded' or 'manifestly excessive', considering a range of factors including (but not limited to) whether the request is repetitive in nature, the nature of the information requested, the context of the request, and the relationship between the Company and the individual making the request. In such cases, it is also possible to request a 'reasonable fee' to handle it, as set out in Part 7.2.

11.1. If either of the above grounds applies, the Company's refusal to comply with the SAR must be justified and an explanation must be provided to the individual making the SAR within one calendar month after receiving the SAR. The individual must also be informed of their right to complain to the Information Regulator.

12. Exemptions to the Right of Access

12.1. Section 23(4)(a) of the Protection of Personal Information Act, read together with chapter 4 of part 3 of the Promotion of Access to Information Act, provides a number of exemptions which apply to SARs and therefore justify the Company refusing to comply with a SAR. Those most likely, but not limited, to be applicable within the Company are situations in which the personal information in question is:

a) subject to legal or litigation privilege; or
b) could jeopardize the privacy of a third party that is a natural person; or
c) relates to commercial information of a third party; or
d) information that could jeopardize the safety of individuals or protection of property.

13. Erasure or Disposal of Personal information

13.1. If any personal information relevant to a SAR is amended, deleted, or otherwise disposed of between the time at which a SAR is received and the time at which a response is made, the Company can take this into account in our response provided that amendment, deletion, or disposal would have been made irrespective of our receipt of the SAR in question.

13.2. The Right of Access does not, therefore, prevent the Company from managing personal information in accordance with normal procedures, in particular those set out in our Protection of Personal Information and Data Retention Policies. It is not, however, permissible to amend, delete, or otherwise dispose of information as an alternative to complying with a SAR.

14. Failure to Comply with this Policy

14.1. Compliance with the Protection of Personal Information Act is of vital importance to the Company. If we fail to comply with a SAR, we will be in breach of our obligations under the Protection of Personal Information Act.

14.2. Failing to comply with the Protection of Personal Information Act may put the data subject at risk. It may also result in the following consequences for the Company:

a) the data subject reporting the Company to the Information Regulator, resulting in an investigation;
b) action taken against the Company which may result in civil and/or criminal sanctions for the Company and, in certain cases, the Information Officer.

14.3. Failure by any member of staff to comply with this Policy may result in disciplinary action which may include dismissal for gross misconduct.

15. Policy Review

This Policy will be reviewed regularly. The Company's Information Officer shall be responsible for reviewing this Policy.

16. Implementation of Policy

This Policy shall be deemed effective as of 1 July 2021. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

POPIA FORMS

ANNEXURE A: FORM SCN1:

NOTIFICATION OF A SECURITY COMPROMISE IN TERMS OF SECTION 22 OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013)

Note:

1. *Attach documents in support of the notification*
2. *Complete the form in full as is applicable*
3. *If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.*

A	**DETAILS OF RESPONSIBLE PARTY**	
Name(s) and Surname / Registered name of responsible party:		
Address:		
	Code ( )	
Contact Number(s):		
E-mail Address:		
B	**DETAILS OF THE INFORMATION OFFICER**	
Full names of information officer		
Registration number of information officer		
Contact Number(s):		
E-mail Address:		
C	**DETAILS OF SECURITY COMPROMISE**	
Date of incident		
Date incident reported to Information Regulator		
Explanation for delay in notification to the Regulator, if applicable		
Type of Security Compromise *(Kindly tick applicable box)*	Loss of personal information	
	Damage to personal information	
	Unauthorised destruction of personal information	
	Unlawful access to of personal information	
	Unlawful processing of personal information	
	Other (please explain):	
Description of Incident:		
Type of Personal Information Compromised: *(Kindly tick applicable box)*	Personal information of children	
	Unique identifiers	
	Special Personal Information	
	Other:	
Number of Data Subjects Affected:		

Method of notification to affected data subjects	Mail to the data subject's last known physical or postal address;	
	Sent by e-mail to the data subject's last known e-mail address;	
	Placed in a prominent position on the website of the responsible party;	
	Published in the news media	
Does the notification provide sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise, including-	A description of the possible consequences of the security compromise;	
	A description of the measures that the responsible party intends to take or has taken to address the security compromise;	
	A recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise;	
	If known, the identity of the unauthorised person who may have accessed or acquired the personal information.	
Status of Compromise	Confirmed	
	Alleged	
D	**DESCRIPTION OF THE MEASURES THAT THE RESPONSIBLE PARTY INTENDS TO TAKE OR HAS TAKEN TO ADDRESS THE SECURITY COMPROMISE AND TO PROTECT THE PERSONAL INFORMATION OF THE DATA SUBJECTS FROM FURTHER UNAUTHORISED ACCESS OR USE.**	
E	**DECLARATION**	

I declare that the information contained herein is true, correct and accurate.

SIGNED at _____on this the _____day of _____20___

_____

Signature

_____ _____

Name **Designation**

FORM 1: OBJECTION TO THE PROCESSING OF PERSONAL INFORMATION

IN TERMS OF SECTION 11(3) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO.4 OF 2013)

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2017, [Regulation 2(1)]

Note:
1. Affidavits or other documentary evidence in support of the objection must be attached.
2. If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.

Reference Number: _____

A	**DETAILS OF DATA SUBJECT**
Name and surname of data subject:	
Residential, postal or business address:	
	Code: ( )
Contact number(s):	
E-mail address:	
B	**DETAILS OF RESPONSIBLE PARTY**
Name of responsible party	
Residential, postal or business address:	
	Code: ( )
Contact number(s):	
E-mail address:	
C	**REASONS FOR OBJECTION** *(Please provide detailed reasons for the objection)*

Signed at _____ on this _____ day of _____ 20_____.

_____
Signature of data subject (applicant)

FORM 2: REQUEST FOR CORRECTION OR DELETION OF PERSONAL INFORMATION OR DESTROYING OR DELETION OF RECORD OF PERSONAL INFORMATION

IN TERMS OF SECTION 24(1) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO.4 OF 2013)

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2017 [Regulation 3(2)]

Note:
1. Affidavits or other documentary evidence in support of the request must be attached.
2. If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.

Reference Number: _____

Mark the appropriate box with an "x".
Request for:

	Correction or deletion of the personal information about the data subject which is in possession or under the control of the responsible party.
	Destroying or deletion of a record of personal information about the data subject which is in possession or under the control of the responsible party and who is no longer authorised to retain the record of information.

A	**DETAILS OF DATA SUBJECT**
Name and surname of data subject:	
Identity Number:	
Residential, postal or business address:	
	Code: ( )
Contact number(s):	
E-mail address:	
B	**DETAILS OF RESPONSIBLE PARTY**
Name responsible party	
Residential, postal or business address:	
	Code: ( )
Contact number(s):	
E-mail address:	
C	**REASON FOR REQUEST** *(Please provide detailed reasons for the request)*

Signed at _____ on this _____ day of _____ 20_____.

_____
Signature of data subject (applicant)

FORM 4: APPLICATION FOR THE CONSENT OF A DATA SUBJECT FOR THE PROCESSING OF PERSONAL INFORMATION FOR THE PURPOSE OF DIRECT MARKETING

IN TERMS OF SECTION 69(2) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013)

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2017, [Regulation 6]

TO: _____
_____
_____
_____
(Name and address of data subject)

FROM: _____
_____
_____
_____

Contact number(s): _____
E-mail address: _____
(Name, address and contact details of responsible party)

Dear Mr/Ms/Dr/Adv/Prof

PART A

1. In terms of section 69 of the Protection of Personal Information Act, 2013 (Act No. 4 of 2013), the processing of personal information of a data subject (the person to whom personal information relates) 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 written consent to the processing is given by the data subject. You may only be approached once for your consent by this responsible party. After you have indicated your wishes in Part B, you are kindly requested to submit this Form either by post, facsimile or e-mail to the address, facsimile number or e-mail address as stated above.
2. "**Processing**" means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including—
   a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
   b) dissemination by means of transmission, distribution or making available in any other form; or
   c) merging, linking, as well as restriction, degradation, erasure or destruction of information.
3. "**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—
   a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
   b) information relating to the education or the medical, financial, criminal or employment history of the person;
   c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
   d) the biometric information of the person;
   e) the personal opinions, views or preferences of the person;
   f) 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;
   g) the views or opinions of another individual about the person; and

h) 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.

_____
(Signature of person authorised by responsible party)

Full names and designation of person signing on behalf of responsible party:

_____

Date: _____

PART B

I, _____(full names of data subject) give my consent to receive direct marketing of goods or services to be marketed by means of electronic communication.

Specify goods or services: _____

Specify method of communication: ☐ Email:
☐ SMS:

Signed at _____ on this _____ day of _____ 20_____.

_____
Signature of Data Subject

DATA BREACH REGISTER			
Company Name:		Date Document Downloaded:	
Registered Address:		Point of Contact:	
Premises Address:			
Data Breach Reference Information			
Data Breach Reference Number:		Data Breach Reported By:	
Time & Date of Data Breach:		Data Breach Handled By:	
Time & Date of Internal Notification of Data Breach:			
Data Breach Details			
Summary of Data Breach:			
Cause of Data Breach:			
Type(s) of Data Affected:			
Type(s) of Personal Information Affected:			
Approximate Number of Data Records Affected:		Type(s) of Data Subject(s) Affected:	
Approximate Number of Data Subjects Affected (if applicable):		Data Breach Reference Number(s) of Any Related Breach or Breaches:	
Further Observations:			

Management of Data Breach			
Impact of Data Breach:			
Severity of Data Breach:			
Initial Containment Measures Taken:			
Initial Notifications (if applicable):			
Data Protection Measures Currently in Place:			
Further Action to be Taken (including preventative measures and other changes):			
Notification			
Has the Information Regulator Been Notified? (provide times, dates, summary details, and reasoning):			
Have Data Subjects Been Notified? (provide times, dates, summary details, and reasoning):			
Have Other Parties Been Notified? (provide times, dates, summary details, and reasoning):			
Additional Comments			
Current Status			
Current Status of Data Breach:		**Date of Current Status:**	

DATA BREACH REPORT FROM (INTERNAL USE)

Important Information

The Company collects, holds, and processes a range of personal information and non-personal information. The protection of this information ("data") is of great importance, both commercially and legally. In the event of a data breach, the Company's Data Breach Policy should be followed. A data breach may include (but not be limited to):

- the loss or theft of a physical data record;
- the loss or theft of computer equipment (e.g. laptop), mobile devices (e.g. smartphone or tablet), portable data storage devices (e.g. USB drive), or other data storage devices;
- equipment failure;
- unauthorised access to, use of, or modification of data (or inadequate access controls allowing unauthorised access, use, or modification);
- unauthorised disclosure of data;
- human error (e.g. sending data to the wrong recipient);
- unforeseen circumstances such as fire or flood;
- hacking, phishing, and other 'blagging" offences whereby information is obtained by deception;

If you discover or suspect a data breach, please complete this Data Breach Report Form and send the completed form to the Company's Information Officer or any of its appointed Deputy Information Officers. If appropriate, you may need to liaise with your line manager when completing this form.

After sending this form, unless and until instructed to by the Company's Information Officer or any of its appointed Deputy Information Officers, you should not take any further action with respect to a data breach. In particular, you must not take it upon yourself to notify affected data subjects, the Information Regulator's Office, or any other individuals or organisations. The Company's Information Officer will determine the steps to be taken to address the data breach, whom to notify, when and how.

Your Details
You may complete and submit this form anonymously. If you wish to do so, please put *anonymous* in each of the fields in this section.

Title:	
Name(s):	
Surname:	
Department (if applicable):	
Manager or supervisor:	
Telephone number:	
Email address:	
Date of this Breach Report:	

Details of Data Breach

Please provide as much detail as you can about the data breach that you have discovered or suspect. The more accurate and specific the information provided in this form, the more quickly and effectively the Company will be able to deal with the data breach.

Date and time of data breach:	
Date and time data breach discovered:	
Is the data breach actual or suspected?	
Please provide a summary of the data breach:	
What type(s) of data are involved?	
Approximately how much data is involved?	
Is personal information involved?	
Is special personal information involved?	
If personal (or special personal) information is involved, what type(s) of information subject are affected (e.g. customers, employees)? (please do not identify any individual data subjects)	
Approximately how many data subjects (if any) are likely to be affected (if known)? (please do not identify any individual data subjects)	
What caused the data breach? (please provide as much detail as you can)	
Have you or any other member of staff taken any action relating to the breach since discovery other than completing this form? (if yes, please provide as much detail as you can)	
Is the data breach ongoing?	
Are you aware of any other data breaches, related or otherwise? (if yes, please provide details)	

For Use by the Information Officer or Deputy Information Officers

Received by:	
Date received:	
Forwarded for action to (if applicable):	
Date forwarded (if applicable):	

PAIA MANUAL