PROMOTION OF ACCESS TO INFORMATION ACT (PAIA) & PROTECTION OF PERSONAL INFORMATION ACT (POPIA) MANUAL

FOR

Bhimma and Partners Inc.

(2014/005516/21)

herein known as “The Company”

C12 Waves Edge, 1004 Otto du Plessis Dr

Bloubergstrand, 7441

PAIA AND POPI POLICY STATEMENT AND MANUAL

This manual was prepared in accordance with Section 51 of the Promotion of Access to Information Act, 2000 ("The Act") and to address requirements of the Protection of Personal Information Act, 2013 ("POPIA") and the Retention of Documents for the Company and all its subsidiaries and divisions (hereinafter referred to as the Company").

INDEX

DOCUMENT MANAGEMENT

DATE	VERSION	DESCRIPTION
30 June 2021	1.0	First Release

1. Introduction

Vision Works Optometrists is a leading Optometry brand in eye health and eye care. This requires The Company to collect, process, and store personal information on a routine basis, obliging The Company to comply with the Protection of Personal Information Act 4 of 2013 ("POPI").

POPI requires The Company to inform their patients as to the manner in which their personal information is used, disclosed and destroyed. The Company is committed to supporting the rights to access to information and the protection of personal information as established in PAIA and POPIA.

This Policy sets out the manner in which The Company deals with their patient's personal information as well as stipulates the purpose for which said information is used.

The Policy is made available by request from The Company store and website.

2. Background and Purpose

2.1. What is the purpose of POPI?

The aim of POPI is to ensure the right of South African citizens to the privacy of personal information and to regulate all organisations that collect, store and utilise personal information.

Personal information may only be processed if the process meets the conditions of the Act. There are eight distinct conditions which organisations need to meet to be acting lawfully:

- Accountability
- Processing limitation
- Purpose specification
- Use limitation
- Information quality
- Openness
- Security safeguards
- Individual/data subject participation

2.2. What is "personal information"?

Personal information means any information relating to an identifiable natural person (and existing juristic persons where applicable), including information relating to:

- Race, gender, sex, pregnancy, marital status, mental health, well-being, disability, religion, belief, culture, language and birth
- Education, medical, financial, criminal or employment
- Identity number, electronic and physical addresses, telephone numbers and on-line identifiers
- Biometric information

- Personal opinions, views or preferences
- Correspondence sent by a person implicitly or explicitly of a personal nature or confidential

An organisation may *not* process the personal information of a child (under 18) unless the processing:

- Is carried out with the consent of the legal guardian
- Is necessary to establish, exercise or defence of a right or obligation in law
- Is necessary for historical, statistical or research purposes
- Is information that is deliberately been made public by the child with the consent of the guardian

2.3. What is processing personal information?

Processing means any operation or activity, or set of activities, by automatic means or otherwise, including:

- Collecting, receiving, recording, collating, storing, updating, modifying, retrieving or use
- Disseminating by means of transmission, distribution or any other means
- Merging, linking, restricting, erasing or destructing of information.

2.4. Who must comply?

All public and private bodies must comply.

2.5. What does compliance mean?

a) Accountability:

Organisations must assign responsibility to ensure compliance with POPI to a suitable person.

Each organisation has an “information officer”. This will be the same person who has been appointed by the organisation as head in terms of the Promotion of Access to Information Act, i.e. the CEO or equivalent. The information officer, together with an executive team/board, should decide on and record the POPI policy and procedure.

The information officer must appoint a “data controller” or a number of data controllers who decide

- the *purpose* of the data processing
- the *way* the personal information should be processed

The data controllers should be management who execute the POPI policy and procedure.

“Data processor/s” perform the processing administration/function (e.g. data capturing etc).

b) Processing limitation

Personal information may only be processed if it is:

- adequate, *relevant and necessary* for the purpose for which it is processed
- with the *consent* of the data subject
- necessary for the *contract* to which the data subject is party
- necessary for the *protection of a legitimate interest* of the data subject
- required by law
- necessary to pursue the *legitimate interest* of the organisation
- *collected directly* from the data subject, except in certain circumstances (e.g. in public domain or to do so would defeat the purpose for collecting and processing)

“Consent” must be:

- voluntary
- specific
- informed

Informed consent requires that the data subject understand:

- *what* information is being collected/processed
- *why* the information is being processed
- how the information is be processed
- *where* the information is being processed
- *to whom* the information is intended to be given

c) Purpose specification

The data subject must be made aware of the purpose for which the information is being collected (“identified purpose”). This is necessary for giving consent (see above).

d) Use limitation

Information/records may only be kept for as long as it is necessary to achieve the identified purpose. There are some statutory record keeping periods which may exceed this. After this *retention* period the responsible person must delete or destroy such information as soon as reasonably possible.

e) Information quality

Information must be as *accurate* as possible, complete and updated if necessary. Information must be available to the data subject to verify/object to the accuracy thereof.

f) Openness

The Organisation must take reasonable practical steps to ensure that the data subject is aware of what personal information is being collected, stored and used, whether or not collected directly from the data subject.

g) Security safeguards

The organisation must secure the integrity and confidentiality of personal information und must take appropriate technical/organisational measure to prevent:

- the loss of or damage to personal information
- the unlawful access to or processing of personal information

To do this, the organisation must:

- identify all reasonable foreseeable internal and external risks to personal information held
- establish and maintain appropriate reasonable safeguards against the risks
- monitor the safeguards and regularly verify safeguards are effective
- ensure safeguards are updated to respond to new risks or deficiencies in previous safeguards

The data controllers and data processors must operate under his/her authority from the information officer and treat all personal information as confidential. This should be in writing.

Where there are reasonable grounds for suspecting a breach of data security, the responsible person must notify the Regulator and the data subject (if known).

h) Data subject participation

Any person who can positively identify themselves is entitled to access or get a copy of their own personal information.

A data subject has the right to correct or amend any of their personal information that may be inaccurate, misleading or out of date.

What steps should be taken to comply?

a) An audit should be conducted of the following:
- *what* personal information is held?
- *where* the personal information is being held?
- *by whom* is the personal information being held?

b) Establish what personal information is being collected in one place and being transferred to another.
c) Review website and other privacy statement (if applicable).
d) Develop organisation wide standard data protection policies and protocols, and if already in place, review such policies and protocols.
e) Review IT outsourcing contracts and arrangements.
f) Review data collecting activities (completion of forms etc.).
g) Appoint an information officer for POPI and PAIA purposes.

2.6. Details of Information Officer

The details of the The Company ‘s Information Officer is as follows:

Information Officer: Avinal Bhimma

Telephone Number: 0836096835

Email Address: avinal@avinalbhimma.co.za

Deputy Information Officer: Kasentrhi Perumal

Telephone Number: 0215562021/27

Email Address:kasuwas@gmail.com

Address: C12 Waves Edge, 1004 Otto du Plessis Dr, Bloubergstrand, 7441

Telephone: 0836096835

Postal Address: Shop 77 Bayside Mall, 75 Blaauwberg Rd, Table View, 7441

3. Personal Information Collected

Section 9 of POPI states that “Personal Information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive.”

The Company collects and processes three main categories of information:

1. The identity and contact details of account holders and patients. This is so that we can make sure we’re dealing with the right person at all times. We may contact you with special offers we think may interest you, but we will never sell this information to anyone else, we will never spam you, and we will quickly remove you from our marketing lists should you choose to opt out.

2. Your medical aid details. This is so that we can claim on your behalf.

3. Patient’s eye health information. This is for us to give you the best quality eye care.

The Company aims to have agreements in place with all product suppliers and third party service providers to ensure a mutual understanding with regard to the protection of the patient’s personal information. The Company suppliers will be subject to the same regulations as applicable to The Company

The Company also collects employee information for staff administration such as attendance and training registers for payroll, SETA etc.

3.1. Categories of Data Subjects and their Personal Information

The Company may possess and supply records relating to suppliers, shareholders, contractors service providers, staff and patients who render the following services:

- Capturing and organising of data;
- Storing of data;
- Sending of emails and other correspondence to patients
- Conducting medical aid benefit authorisation checks;
- Administration of the debt collection;

Entity Type	**Personal Information Processed**
Patients – Juristic Persons / Entities	Names of contact persons; Name of Legal Entity; Physical and Postal address and contact details
Patients – Natural Persons	Names; contact details; physical and postal addresses; medical information; refractive information; preferences regarding optical correction; confidential correspondence
Intermediary / Advisor	Names of contact persons; Name of Legal Entity; Physical and Postal address and contact details
Contracted Service Providers	Names of contact persons; Name of Legal Entity; Physical and Postal address and contact details.
Employees / Directors	Gender, Pregnancy; Marital Status; Race, Biometric information, Age, Language, Education information; Financial Information; Employment History; ID number; Physical and Postal address; Contact details; Opinions, Criminal behaviour; Well-being

3.2. Actual or Planned Trans-border Flows of Personal Information

The Company may transfer data trans-border in order to store data with third party cloud storage providers.

3.2.1. Section 72 of POPIA provides that Personal Information may only be transferred out of the Republic of South Africa if the:

a) Recipient country can offer such data an “adequate level” of protection. This means that its data privacy laws must be substantially similar to the Conditions for Lawful Processing as contained in POPI; or
b) Data Subject consents to the transfer of their Personal Information; or
c) Transfer is necessary for the performance of a contractual obligation between the Data Subject and the Responsible Party; or

d) Transfer is necessary for the performance of a contractual obligation between the Responsible Party and a third party, in the interests of the Data Subject; or
e) The transfer is for the benefit of the Data Subject, and it is not reasonably practicable to obtain the consent of the Data Subject, and if it were, the Data Subject, would in all likelihood provide such consent.

3.3. Objection to the Processing of Personal Information by a Data Subject

Section 11 (3) of POPI and regulation 2 of the POPIA Regulations provides that a Data Subject may, at any time object to the Processing of his/her/its Personal Information in the prescribed form attached to this manual as Appendix 1 subject to exceptions contained in POPIA.

3.4. Request for correction or deletion of Personal Information

Section 24 of POPI and regulation 3 of the POPI Regulations provides that a Data Subject may request for their Personal Information to be corrected/deleted in the prescribed form attached as Appendix 2 to this Manual.

3.5. General Description of Information Security Measures

The Company employs up to date technology to ensure the confidentiality, integrity and availability of the Personal Information under its care. Measures include:

- Firewalls
- Virus protection software and update protocols
- Logical and physical access control;
- Secure setup of hardware and software making up the IT infrastructure;
- Outsourced Service Providers who process Personal Information on behalf of The Company are contracted to implement security controls.
- Windows 10 on all computers

4. The Use of Personal Information

The Patient's Personal Information by The Company will only be used for the purpose for which it was collected and as agreed. This may include:

4.1 According to section 10 of POPI, personal information may only be processed if certain conditions, listed below, are met along with supporting information for The Company processing of Personal Information:

4.1.1. The patient's consents to the processing: - consent is obtained from patients during the initial visit prior to the appointment (medical aid benefit confirmation), and the day of the appointment;

4.1.2. The necessity of processing: in order to conduct an accurate analysis of the patient's needs

4.1.3. Processing complies with an obligation imposed by law on The Company;

4.1.4. Processing protects a legitimate interest of the patient

4.1.5. Processing is necessary for pursuing the legitimate interests of The Company or of a third party (referral health care professionals/medical aid/insurance companies) to whom information is supplied — in order to provide The Company patients with products and or services both The Company and any of our product suppliers require certain personal information from the patients in order to make an expert decision on the unique and specific product and or service required.

4.2 Providing products or services to patients and to carry out the transactions requested;
4.3 Confirming, verifying and updating patient details;
4.4 Conducting market or customer satisfaction research;
4.5 Relevant points of contact throughout the product purchase cycle and after sales service/recall;
4.6 For audit and record keeping purposes;
4.7 In connection with legal proceedings;
4.8 Providing services to patients, to render the services requested and to maintain and constantly improve the relationship;
4.9 Providing communication in respect of The Company and regulatory matters that may affect patients;
4.10 In connection with and to comply with legal and regulatory requirements or when it is otherwise allowed by law;

5. Disclosure of Personal Information

5.1. The Company may disclose a patient's personal information to any of the The Company subsidiaries, and or approved product supplier or third party service providers whose services or products patients elect to use. The Company has agreements in place to ensure compliance with confidentiality and privacy conditions.
5.2. The Company may also share patient personal information with, and obtain information about patients from third parties for the reasons already discussed above.
5.3. The Company may also disclose a patient's information where it has a duty or a right to disclose in terms of applicable legislation, the law, or where it may be deemed necessary in order to protect The Company rights.
5.4. All employees have a duty of confidentiality in relation to The Company and patients.
5.5. Information on patients: Our patients' right to confidentiality is protected in the Constitution and in terms of the Law. Information may be given to a third party if the patient has consented in writing to that person receiving the information.
5.6. The Company views any contravention of this policy very seriously and employees who are guilty of contravening the policy will be subject to disciplinary procedures, which may lead to the dismissal of any guilty party.
5.7. Disclosure to third parties: All employees have a duty of confidentiality in relation to The Company and patients. Information on patients: Our patients' right to confidentiality is protected in the Constitution and in terms of the Electronic Communications and Transaction Act, 25 of 2002. Information may be given to a third party if the patient has consented in writing to that person receiving the information.

6. Safeguarding Personal Information

6.1. It is a requirement of POPI to adequately protect personal information. The Company will continuously review its security controls and processes.

6.2. The Company Information Officer's details are available above, is responsible for the compliance with the conditions of the lawful processing of personal information and other provisions of POPI.
6.3. This policy has been put in place throughout The Company and training on this policy and the POPI Act has already taken place and will be conducted during 2021 by The Company.
6.4. Each new employee will be required to sign an Employment Contract containing relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of POPI;
6.5. Every employee currently employed within The Company will be required to sign an addendum to their Employment Contracts containing relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of POPI;
6.6. All The Company electronic files or data are backed up and stored off site. IT providers are also responsible for system security to protect against third party access and physical threats;
6.7. The Companies product suppliers, insurers and other third-party service providers will be required to sign a service level agreement guaranteeing their commitment to the Protection of Personal Information; this is however an ongoing process that will be evaluated as needed.
6.8. The Companies archived patient information is stored both on and off site is also governed by POPI. Access is limited to these areas to authorized personnel only.
6.9. Consent to process patient information is obtained from patients (or a person who has been given authorization from the patient to provide the patient's personal information) during the registration, appointment and needs analysis stage of the relationship.

7. Access and Correction of Personal Information

Patients have the right to access the personal information The Company holds about them. Patients also have the right to ask The Company to update, correct or delete their personal information on reasonable grounds. Once a patient objects to the processing of their personal information, The Company may no longer process said personal information. The Company will take all reasonable steps to confirm its patients' identity before providing details of their personal information or making changes to their personal information.

8. Amendments to this Policy

Amendments to, or a review of this Policy, will take place on an ad hoc basis or at least once a year. Patients are advised to access The Company's website periodically to keep abreast of any changes. Where material changes take place, patients will be notified directly or changes will be stipulated on The Company website.

9. Access to Documents

All Company and patient information must be dealt with in the strictest confidence and may only be disclosed, without fear of redress, in the following circumstances:

9.1. where disclosure is under compulsion of law;
9.2. where there is a duty to the public to disclose;
9.3. where the interests of The Company require disclosure; and
9.4. where disclosure is made with the express or implied consent of the patient.

10. Requests for The Company Information

10.1. These are dealt with in terms of the Promotion of Access to Information Act, 2 of 2000 ("PAIA"), which gives effect to the constitutional right of access to information held by the State or any person (natural and juristic) that is required for the exercise or protection of rights. Private bodies, like The Company, must however refuse access to records if disclosure would constitute an action for breach of the duty of secrecy owed to a third party.

10.2. In terms hereof, requests must be made in writing on the prescribed form to the Information Officer in terms of PAIA. The requesting party has to state the reason for wanting the information and has to pay a prescribed fee.

Request Procedure

A requester (personal or other) must comply with all the procedural requirements contained in the Act relating to a request for access to a record. A requester must complete the prescribed form enclosed herewith in Appendix 3 and submit same as well as payment of a request fee and a deposit, if applicable to the information officer at the postal or physical address, fax number or electronic mail address stated herein. The prescribed form must be filled in with enough particularity to at least enable the information officer to identify:

- The record or records requested;
- The identity of the requester;
- What form of access is required; and
- The postal address or e-mail address of the requester.

A requester must state that he or she requires the information in order to exercise or protect a right, and clearly state what the nature of the right is so to be exercised or protected. The requester must also provide an explanation of why the requested record is required for the exercise or protection of that right.

The Company will process a request within 30 days, unless the requestor has stated special reasons which would satisfy the information officer that circumstances dictate that the time period not be complied with. The requester shall be informed in writing whether access has been granted or denied. If, in addition, the requester requires the reasons for the decision in any other manner, he or she must state the manner and the particulars so required. If a request is made on behalf of another person, the requester must then submit proof of the capacity in which the requester is making the request to the satisfaction of the information officer.

If an individual is unable to complete the prescribed form because of illiteracy or disability, such a person may make the request orally to the information officer.

Decision

The Company will, within 30 days of receipt of a request, decide whether to grant or decline a request and give notice with reasons (if required) to that effect. The 30 day period within which The Company has to decide whether to grant or refuse a request, may be extended for a further period

of not more than 30 days if the request is for a large quantity of information, and the information cannot reasonably be obtained within the original 30 day period. The information officer will notify the requester in writing should an extension be necessary.

Fees

The Act provides for two types of fees:

A request fee, (which will be a standard fee) and an access fee, which must be calculated by taking into account reproduction costs, search and preparation time and cost, as well as postal costs where applicable. When a request is received by the information officer of the Company, the information officer shall by notice require the requester, other than a personal requester, to pay the prescribed request fee (if any), before further processing of the request. If a search for the record is necessary and the preparation of the record for disclosure, including arrangement to make it available in the requested form, requires more than the hours prescribed in the regulations for this purpose, the information officer shall notify the requester to pay as a deposit the prescribed portion of the access fee which would be payable if the request is granted.

The information officer shall withhold a record until the requester has paid the fee or fees as indicated. A requester whose request for access to a record has been granted, must pay an access fee for reproduction and for search and preparation, and for any time reasonably required in excess of the prescribed hours to search for and prepare the record for disclosure including making arrangements to make it available in the request form. If a deposit has been paid in respect of a request for access, which is refused, then the information officer shall repay the deposit to the requester.

Fees Provided by the Act

The Act provides for two types of fees, namely:

a) A request fee, which is a form of administration fee to be paid by all requesters except personal requesters, before the request is considered and is not refundable; and
b) An access fee, which is paid by all requesters in the event that a request for access is granted. This fee is inclusive of costs involved by the private body in obtaining and preparing a record for delivery to the requester.

When the request is received by the Information Officer, such officer shall by notice require the requester, other than a personal requester, to pay the prescribed request fee, before further processing of the request (section 54(1)).

If the search for the record has been made and the preparation of the record for disclosure, including arrangement to make it available in the requested form, requires more than the hours prescribed in the regulations for this purpose, the Information Officer shall notify the requester to pay as a deposit the prescribed portion of the access fee which would be payable if the request is granted

The Information Officer shall withhold a record until the requester has paid the fees as indicated below.

A requester whose request for access to a record has been granted, must pay an access fee that is calculated to include, where applicable, the request fee, the process fee for reproduction and for search and preparation, and for any time reasonably required in excess of the prescribed hours to search for and prepare the record for disclosure including making arrangements to make it available in the request form.

If a deposit has been paid in respect of a request for access, which is refused, then the Information Officer concerned must repay the deposit to the requester.

Reproduction Fee

Where The Company has voluntarily provided the Minister with a list of categories of records that will automatically be made available to any person requesting access thereto, the only charge that may be levied for obtaining such records, will be a fee for reproduction of the record in question.

Reproduction of Information Fees	Fees to be Charged
Information in an A-4 size page photocopy or part thereof	R 1,10
A printed copy of an A4-size page or part thereof	R 0,75
A copy in computer-readable format, for example: Compact disc	R 70,00
A transcription of visual images, in an A4-size page or part thereof	R 40,00
A copy of visual images	R 60,00
A transcription of an audio record for an A4-size page or part thereof	R 20,00
A copy of an audio record	R 30,00

Request Fees

Where a requester submits a request for access to information held by an institution on a person other than the requester himself/herself, a request fee in the amount of R50,00 is payable up-front before the institution will further process the request received.

Access Fees

An access fee is payable in all instances where a request for access to information is granted, except in those instances where payment of an access fee is specially excluded in terms of the Act or an exclusion is determined by the Minister in terms of section 54(8).

The applicable access fees which will be payable are: **Access of Information Fees**	Fees to be Charged
Information in an A-4 size page photocopy or part thereof	R 1,10
A printed copy of an A4-size page or part thereof	R 0,75
A copy in computer-readable format, for example:	R 7,50

Stiffy disc Compact disc	R 70,00
A transcription of visual images, in an A4-size page or part thereof	R 40,00
A copy of visual images	R 60,00
A transcription of an audio record for an A4-size page or part thereof	R 20,00
A copy of an audio record *Per hour or part of an hour reasonably required for such search.	R 30,00*

Where a copy of a record needs to be posted the actual postal fee is payable.

Deposits

Where the institution receives a request for access to information held on a person other than the requester himself/herself and the Information Officer upon receipt of the request is of the opinion that the preparation of the required record of disclosure will take more than 6 (six) hours, a deposit is payable by the requester.

The amount of the deposit is equal to 1/3 (one third) of the amount of the applicable access fee.

Collection Fees

The initial "request fee" of R50,00 should be deposited into the bank account below and a copy of the deposit slip, application form and other correspondence / documents, forwarded to the Information Officer via fax.

The officer will collect the initial "request fee" of applications received directly by the Information Officer via email.

All fees are subject to change as allowed for in the Act and as a consequence such escalations may not always be immediately available at the time of the request being made. Requesters shall be informed of any changes in the fees prior to making a payment.

10.3. Requests for company information: These are dealt with in terms of the Promotion of Access to Information Act, 2 of 2000 (PAIA), which gives effect to the constitutional right of access to information held by the State or any person (natural and juristic) that is required for the exercise or protection of rights. Private bodies, like the Company, must however refuse access to records if disclosure would constitute an action for breach of the duty of secrecy owed to a third party.

10.4. The Companies manuals in terms of PAIA, which contains the prescribed forms and details of prescribed fees is available on request.

A copy of this Manual is available:

- At our reception desk at our practice (address on the cover page)
- On request from our Information Officer
- On our website: www.vision-works.co.za

This Manual will be updated from time to time, as and when required.

10.5. Confidential company and/or business information of The Company may not be disclosed to third parties as this could constitute industrial espionage. The affairs of The Company must be kept strictly confidential at all times.

Categories Of Records Held By The Company: Section 51(1)(E)

We hold records in the categories listed below. **The fact that we list a record type here** does not necessarily mean that we will disclose such records, and all access is subject to the evaluation processes outlined herein, which will be exercised in accordance with the requirements of the Act.

Companies Act Records, which includes documents of incorporation, names of directors, minutes of board of directors meetings, records relating to the appointment of directors / auditor / secretary / public officer and other officers, share Register and other statutory registers

Internal records relating to our business, which includes our business's founding and other documents, minutes and policies; annual and other reports; financial records; operational records, policies and procedures; contracts; licences, trademarks and other intellectual property; production, marketing records; other internal policies and procedures; internal correspondence; statutory records; insurance policies and records; etc.

Personnel records, which includes records relating to temporary employees, fixed term employees, part-time employees, permanent employees, locums, associates, contractors, partners, directors, executive directors, non-executive directors. It includes personal files and similar records, records a third parties have provided to us about their personnel; employment contracts, conditions of employment; workplace policies; payroll/salary information, disciplinary records; termination records; minutes of staff meetings; performance management records and systems and all employment-related records and correspondence.

Patient/patient records, which includes patient/patient lists; health records; medical reports; funding records; agreements; consents; needs assessments; financial and accounts information; research information; evaluation records; profiling; and similar information. It must be noted that, in the health sector, personal and patient information are protected by legislation and ethical rules, and disclosure can only take place, if at all, without those frameworks.

Supplier and service provider records, which includes supplier registrations; contracts; confidentiality agreements and non-disclosure agreements, communications; logs; delivery records; commissioned work; and similar information, some of which might be provided to us by such suppliers and providers under service- and other contacts. Technical records, which includes manuals, logs, electronic and cached information, product registrations, product dossiers, health professionals council / statutory body records, approvals, conditions and requirements, trade association information and similar product information.

Third party information, which may be in our possession but which would be subject to the conditions set in relation to such possession and use or purpose limitations.

Environment and market information, which includes information bought, publicly available information and commissioned information which pertains to the specific sector and market of our business and factors that affect the business, professional and healthcare environment.

Financial Records, which includes annual financial statements, tax returns, accounting records, banking records, bank statements, electronic banking records, asset register, rental agreements, invoices, annual financial reports/statements, debtors/creditors statements and invoices.

Tax Records, which includes PAYE records, documents issued to employees for income tax purposes, records of payments made to SARS on behalf of employees all other statutory compliances: VAT, Skills Development Levies, UIF etc.

Note that the accessibility of the records may be subject to the grounds of refusal set out in this PAIA manual. Amongst other, records deemed confidential on the part of a third party, will necessitate permission from the third party concerned, in addition to normal requirements, before The Company will consider access.

11. Voluntary Disclosure

The following information is made known automatically such as promotional terms and conditions forms, brochures, leaflets, etc. and where such documents are available, persons do not have to request such information.

12. Refusal of Access to Records

12.1. Grounds to Refuse Access

A private body is entitled to refuse a request for information.

12.1.1. The main grounds for The Company to refuse a request for information relates to the:

a) mandatory protection of the privacy of a third party who is a natural person or a deceased person (section 63) or a juristic person, as included in the Protection of Personal Information Act 4 of 2013, which would involve the unreasonable disclosure of personal information of that natural or juristic person;
b) mandatory protection of personal information and for disclosure of any personal information to, in addition to any other legislative, regulatory or contractual agreements, comply with the provisions of the Protection of Personal Information Act 4 of 2013;
c) mandatory protection of the commercial information of a third party (section 64) if the record contains:
    i. trade secrets of the third party;

ii. financial, commercial, scientific or technical information which disclosure could likely cause harm to the financial or commercial interests of that third party;
iii. information disclosed in confidence by a third party to The Company, if the disclosure could put that third party at a disadvantage in negotiations or commercial competition;

d) mandatory protection of confidential information of third parties (section 65) if it is protected in terms of any agreement;
e) mandatory protection of the safety of individuals and the protection of property (section 66);
f) mandatory protection of records which would be regarded as privileged in legal proceedings (section 67).

12.1.2. The commercial activities (section 68) of a private body, such as The Company, which may include:

a) trade secrets of The Company;
b) financial, commercial, scientific or technical information which disclosure could likely cause harm to the financial or commercial interests of The Company;
c) information which, if disclosed could put The Company at a
d) disadvantage in negotiations or commercial competition;
e) a computer program which is owned by The Company, and which is protected by copyright;
f) the research information (section 69) of The Company or a third party, if its disclosure would disclose the identity of The Company, the researcher or the subject matter of the research and would place the research at a serious disadvantage.

12.1.3. Requests for information that are clearly frivolous or vexatious, or which involve an unreasonable diversion of resources shall be refused.
12.1.4. All requests for information will be assessed on their own merits and in accordance with the applicable legal principles and legislation.
12.1.5. If a requested record cannot be found or if the record does not exist, the Information Officer shall, by way of an affidavit or affirmation, notify the requester that it is not possible to give access to the requested record. Such a notice will be regarded as a decision to refuse a request for access to the record concerned for the purpose of the Act. If the record should later be found, the requester shall be given access to the record in the manner stipulated by the requester in the prescribed form, unless the Information Officer refuses access to such record.

13. Remedies Available When The Company Refuses a Request

13.1. Internal Remedies

The Company does not have internal appeal procedures. The decision made by the Information Officer is final. Requesters will have to exercise such external remedies at their disposal if the request for information is refused, and the requestor is not satisfied with the answer supplied by the Information Officer.

13.2. External Remedies

13.2.1. A requestor that is dissatisfied with the Information Officer's refusal to disclose information, may within 30 (thirty) days of notification of the decision, may apply to a Court for relief.
13.2.2. A third party dissatisfied with the Information Officer's decision to grant a request for information, may within 30 (thirty) days of notification of the decision, apply to a Court for relief.

For purposes of the Act, the Courts that have jurisdiction over these applications are the Constitutional Court, the High Court or another court of similar status and a Magistrate's Court designated by the Minister of Justice and Constitutional Development and which is presided over by a designated Magistrate.

14. The Company Information Process Flow

The collection, storage, access and dissemination of personal information is set out in Appendix 4.

15. Retention of Documents

15.1. Hard Copy

The statutory periods for the retention of documents are as per the Law. These are available on request.

15.2. Electronic Storage
15.2.1. The internal procedure requires that electronic storage of information: important documents and information must be referred to and discussed with IT who will arrange for the indexing, storage and retrieval thereof. This will be done in conjunction with the departments concerned.
15.2.2. Scanned documents: If documents are scanned, the hard copy must be retained for as long as the information is used or for 1 year after the date of scanning, with the exception of documents pertaining to personnel. Any document containing information on the written particulars of an employee, including: employee’s name and occupation, time worked by each employee, remuneration and date of birth of an employee under the age of 18 years; must be retained for a period of 3 years after termination of employment.
15.2.3. Section 51 of the Electronic Communications Act No 25 of 2005 requires that personal information and the purpose for which the data was collected must be kept by the person who electronically requests, collects, collates, processes or stores the information and a record of any third party to whom the information was disclosed must be retained for a period of 1 year or for as long as the information is used. It is also required that all personal information which has become obsolete must be destroyed.

16. Destruction of Documents

16.1. Documents may be destroyed after the termination of the retention period specified in terms of the Law and HPCSA (Health Professions Council of South Africa). Registration will request departments to attend to the destruction of their documents and these requests shall be attended to as soon as possible.

16.2. Each department is responsible for attending to the destruction of its documents, which must be done on a regular basis. Files must be checked in order to make sure that they may be destroyed and also to ascertain if there are important original documents in the file. Original documents must be returned to the holder thereof, failing which, they should be retained by The Company pending such return.

16.3. The documents are then made available for collection by the removers of the Company's documents, who also ensure that the documents are shredded before disposal. This also helps to ensure confidentiality of information.

16.4. Documents may also be stored off-site, in storage facilities approved by the Company.

Appendix 1 – Objection to processing of personal information

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)

Note:

1. *Affidavits or other documentary evidence as applicable in support of the objection may 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.*
3. *Complete as is applicable.*

A	**DETAILS OF DATA SUBJECT**
Name(s) and surname/ registered name of data subject:	
Unique Identifier/ Identity Number	
Residential, postal or business address:	Code ( )
Contact number(s):	
E-mail address:	
B	**DETAILS OF RESPONSIBLE PARTY**
Name(s) and surname/ Registered name of responsible party:	
Residential, postal or business address:	Code ( )
Contact number(s):	
E-mail address:	
C	**REASONS FOR OBJECTION IN TERMS OF SECTION 11(1) (d) to (f)** *(Please provide detailed reasons for the objection)*

Signed at ..... this ..... day of .....20……..

.....

Signature of data subject/designated person

Appendix 2 - Request for correction or deletion of personal information or destroying or deletion of record of personal information

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

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 THE DATA SUBJECT**
Name(s) and surname / registered name of data subject:	
Unique identifier/ Identity Number:	
Residential, postal or business address:	
	Code ( )
Contact number(s):	
E-mail address:	
B	**DETAILS OF RESPONSIBLE PARTY**
Name(s) and surname / registered name of responsible party:	
Residential, postal or business address:	
	Code ( )
Contact number(s):	
E-mail address:	
C	**INFORMATION TO BE CORRECTED/DELETED/ DESTRUCTED/ DESTROYED**
REASONS FOR *CORRECTION OR DELETION OF THE PERSONAL INFORMATION ABOUT THE DATA SUBJECT IN TERMS OF SECTION 24(1)(a) WHICH IS IN POSSESSION OR UNDER THE CONTROL OF THE RESPONSIBLE PARTY ; and or REASONS FOR *DESTRUCTION OR DELETION OF A RECORD OF PERSONAL INFORMATION ABOUT THE DATA SUBJECT IN TERMS OF SECTION 24(1)(b) WHICH THE RESPONSIBLE PARTY IS NO LONGER AUTHORISED TO RETAIN. *(Please provide detailed reasons for the request)*	

Signed at ..... this ..... day of .....20……..

.....

Signature of data subject/ designated person

Appendix 3 – Request for Access to record of Private Body

(Section 53(1) of the Promotion of Access to Information Act, 2000

(Act No. 2 of 2000)

[Regulation 10]

A. Particulars of private body

The Head:

B. Particulars of person requesting access to the record

(a)	The particulars of the person who requests access to the record must be given below.
(b)	The address and/or fax number in the Republic to which the information is to be sent must be given.
(c)	Proof of the capacity in which the request is made, if applicable, must be attached.

Full names and surname:

Identity number:

Postal address:

Fax number:

Telephone number: E-mail address:

Capacity in which request is made, when made on behalf of another person:

C. Particulars of person on whose behalf request is made

This section must be completed *ONLY if* a request *for information is* made on behalf of *another* person.

Full names and surname:

Identity number:

D. Particulars of record

(a)	Provide full particulars of the record to which access is requested, including the reference number if that is known to you, to enable the record to be located.
(b)	If the provided space is inadequate, please continue on a separate folio and attach it to this form. The requester must sign all the additional folios.

1 Description of record or relevant part of the record:

2 Reference number, if available:

3 Any further particulars of record:

E. Fees

(a)	A request for access to a record, other *than* a record containing personal information about yourself, will be processed only after a request fee has been paid.
(b)	You will be *notified of* the amount required to be paid as the request fee.
(c)	The fee payable for access to a record depends *on* the form *in which* access is required and the reasonable time *required* to search for and prepare a record.
(d)	If you qualify for exemption *of* the payment *of* any fee, please state the reason for exemption.

Reason for exemption from payment of fees:

F. Form of access to record

If you are prevented by a disability to read, view or listen to the record in the form of access provided for in 1 to 4 hereunder, state your disability and indicate in which form the record is required.

Disability:	Form in which record is required
Mark the appropriate box with an X. NOTES: (a) Compliance with your request in the specified form may depend on the form in which the record is available. (b) Access in the form requested may be refused in certain circumstances. In such a case you will be informed if access will be granted in another form. (c) The fee payable for access for the record, if any, will be determined partly by the form in which access is requested.	

1. If the record is in written or printed form:					
	copy of record*		inspection of record		
2. If record consists of visual images this includes photographs, slides, video recordings, computer-generated images, sketches, etc)					
	view the images		copy of the images"		transcription of the images*

3. If record consists of recorded words or information which can be reproduced in sound:					
	listen to the soundtrack audio cassette		transcription of soundtrack* written or printed document		
4. If record is held on computer or in an electronic or machine-readable form:					
	printed copy of record*		printed copy of information derived from the record"		copy in computer readable form* (stiffy or compact disc)

'If you requested a copy or transcription of a record (above), do you wish the copy or transcription to be posted to you? Postage is payable.	YES	NO

G Particulars of right to be exercised or protected

If the provided space is inadequate, please continue on a separate folio and attach it to this form. The requester must sign all the additional folios.

1. Indicate which right is to be exercised or protected:

2. Explain why the record requested is required for the exercise or protection of the aforementioned right:

H. Notice of decision regarding request for access

You will be notified in writing whether your request has been approved/denied. If you wish to be informed in another manner, please specify the manner and provide the necessary particulars to enable compliance with your request.

How would you prefer to be informed of the decision regarding your request for access to the record?

Signed at…… This…… day of ……20

……

SIGNATURE OF REQUESTER / PERSON ON

WHOSE BEHALF REQUEST IS MADE

Appendix 4 – The Company information process flow