Promotion of Access to Information Act

# PAIA MANUAL

PREPARED IN TERMS OF SECTION 51 OF THE PROMOTION OF ACCESS TO INFORMATION ACT 2 of 2000



# 1. Introduction

**Richbam Investment Holdings (Pty) Ltd.**

trading as RIH Training Institute conducts a business specialising in:

- RIH Training Institute provided specialised technical training for local rural yourth..

# 2. Company Contact Details

*Section 51(1)(a)*

| | |
|---|---|
| Name of Business: | Richbam Investment Holdings (Pty) Ltd. |
| Reg. Number: | 2018/204169/07 |
| Industry: | Education |
| Directors: | Benny Maphanga |
| | |
| Contact Person: | Benny Maphanga |
| Physical Address: | No. 3 Bothashoek Road, Mashamotane, |
| Postal Address: | 1150 |
| Telephone: | +27 71 348 1720 |
| Fax: | |
| E-mail: | richbaminvestment@gmail.com |
| Last update: | 12/23/2025 16:48:39 |

# 3. The Act

*Section 51(1)(b)*

The Promotion of Access to Information Act 2 of 2000 grants a requester access to records of a private body, if the record is required for the exercise or protection of any rights. If a public body lodges a request, the public body must be acting in the public interest.

Requests in terms of the ACT shall be made in accordance with the prescribed procedures, at the rates provided. The forms and tariff are dealt with in paragraphs 6 and 7 of the Act.

Requesters are referred to the Guide in terms of Section 10 which has been compiled by the South African Human Rights Commission, which will contain information for the purposes of exercising Constitutional Rights. The Guide is available from the South African Human Rights Commission. Please direct queries to:

**The South African Human Rights Commission:**

**PAIA Unit**

The Research and Documentation Department

| | |
|---|---|
| Postal Address: | Private Bag 2700 Houghton 2041 |
| Telephone: | +27 11 477-3600 |
| Fax: | +27 11 403-0625 |
| Website: | www.sahrc.org.za |
| E-mail: | PAIA@sahrc.org.za |

# 4. Applicable Legislation

*Section 51(1)(c)*

### 4.1 Information is available in terms of the following legislation, if and where applicable:

- Basic Conditions of Employment Act No. 75 of 1997
- Broad-Based Economic Empowerment Act No. 53 of 2003
- Closed Corporation Act No. 69 of 1984
- Companies Act No. 61 of 1973
- Company Act No.98 of 1978
- Compensation for Occupational Injuries and Diseases Act No. 130 of 1993
- Constitution of the Republic of South Africa No.3 of 1994
- Electronic Communications and Transactions Act No. 25 of 2002
- Employment Equity Act No. 55 of 1998
- Financial Intelligence Centre Act No. 38 of 2001
- Hazardous Substances Act No. 15 of 1973
- Income Tax Act No. 58 of 1962
- Information Act No. 70 of 2002.
- Manpower Training Act No. 56 of 1981
- Labour Relations Act No. 66 of 1995
- National Environment Management Act No. 107 of 1998
- Occupational Health and Safety Act No. 85 of 1993
- Prevention of Combating of Corrupt Activities Act No. 12 of 2004
- Prevention of Organised Crime Act No. 121 of 1998
- Promotion of Access to Information Act No. 2 of 2000
- Promotion of Equality and Prevention of Unfair Discrimination Act No. 4 of 2000
- Protected Disclosures Act No. 26 of 2000
- Regulation of Interception of Communications and Provision of Communications
- Skills Development Act No. 97 of 1998
- Skills Development Levies Act No. 9 of 1999
- South African Revenue Services Act, 34 of 1997
- Unemployment Insurance Act No. 30 of 1966
- Unemployment Insurance Contributions Act No. 4 of 2002
- Unemployment Insurance Fund Act No. 63 of 2001
- Value – Added Tax Act No. 89 of 1991

### 4.2 Business specific Legislation:

- 1. The Skills Development Act (SDA) 2. The National Qualifications Framework (NQF) Act 3. The Occupational Health and Safety (OHS) Act 4. The Promotion of Access to Information Act (PAIA) 5. Continuing Education and Training (CET) Act

# 5. Schedule of Records

*Section 51(1)(d)*

Records which are available without a person having to request access in terms of this Act in terms of section 52(2) [Section 51(1)(c)] include details about our products, services, and acceptable use policy.

- Training Material, Marketing material, including social media posts.

Day to day operational information is generally not applicable to persons outside the company for the purpose of protecting their constitutional rights.

Examples of such information are:

- Student records and results.

Details of products / services / acceptable use policy are freely available to the general public on our website (if available) or as a hardcopy manual at No. 3 Bothashoek Road, Mashamotane,.

Clients automatically have direct and full access to all information pertaining to the service / product delivered to them.

# 6. Protection of Privacy

*Protection of Personal Information Act 4 of 2013*

**Protection of Personal Information in terms of POPIA**

The purpose of the Protection of Personal Information Act (POPIA) is to protect people from harm by protecting their personal information, in short to protect their privacy, which is a fundamental human right.

To achieve this, the Protection of Personal Information Act sets conditions for when it is lawful for someone to process someone else's personal information.

In terms of POPIA, personal information must be processed for a specified purpose. The purpose for which data is processed by the Private body 's will depend on the nature of the data and the particular data subject. This purpose is ordinarily disclosed, explicitly or implicitly, at the time the data is collected.

*Please also refer to the Business's Privacy Policy www.rihtraining.co.za/privacy-policy.html for further information.*

### 6.1 RIH Training Institute processes personal information of data subjects

*For the purposes of Sec 51 (1)(c)(i)*

- Fulfilling its statutory obligations in terms of applicable legislation;
- Verifying information provided to RIH Training Institute;
- Obtaining information necessary to provide contractually agreed services to a customer;
- Monitoring, maintaining and managing RIH Training Institute's contractual obligations to customers, clients, suppliers, service providers, employees, directors and other third parties;
- Marketing and advertising;
- Resolving and tracking complaints;
- Monitoring and securing the assets, employees and visitors to the premises of RIH Training Institute;
- Historical record keeping, research and recording statistics necessary for fulfilling RIH Training Institute's business objectives.

### 6.2 RIH Training Institute may process the personal information

*Of the following categories of data subjects, which includes current, past and prospective data subjects: Sec 51 (1)(c)(ii)*

- Customer and employees, representatives, agents, contractors and service providers of such customers;
- Suppliers, service providers to and vendors of RIH Training Institute and employees, representatives, agents, contractors and service providers of such suppliers and service providers;
- Directors and officers of RIH Training Institute;
- Shareholders;
- Job applicants;
- Existing and former employees (including contractors, agents, temporary and casual employees);
- Visitors to any premises of RIH Training Institute; and
- Complaints, correspondence, and enquiries.

### 6.3 The nature of personal information processed

*In respect of the above data subjects may include, as may be applicable: Sec 51 (1)(c)(ii)*

- Name, identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
- Biometric information;
- Information relating to the education or the medical, financial, criminal or employment history of the data subject;
- Information relating to the rate, gender, marital status, national origin, age disability, language and birth of the data subject;
- The personal opinions, views or preferences of the data subject;
- Confidential correspondence sent by the data subject;
- The views of opinions of another individual about the data subject.

### 6.4 RIH Training Institute may supply personal information

*To the following recipients: Sec 51 (1)(c)(iii)*

- Regulatory, statutory and government bodies;
- Suppliers, service providers, vendors, agents and representatives of RIH Training Institute;
- Employees of RIH Training Institute;
- Shareholders and other stakeholders;
- Third party verification agencies and credit bureau;
- Collection agencies;
- Banks and other financial institutions.

### 6.5 Planned or prospective transborder flow of personal information

*Processed by RIH Training Institute in respect of the above categories of data subjects: Sec 51 (1)(c)(iv)*

Personal information of data subjects may be transferred across borders due to the hosting of some RIH Training Institute infrastructure and application in foreign jurisdictions.

Current employees and consultants' information may also be transferred transborder where RIH Training Institute has a physical presence or may be providing services or performing in terms of its contractual obligations.

### 6.6 Security measures (to be) implemented by RIH Training Institute

*To ensure the confidentiality, integrity and availability for the personal information which may be or is being processed by RIH Training Institute: Sec 51 (1)(c)(v)*

RIH Training Institute continuously establishes and maintains appropriate, reasonable technical and organisational measures to ensure that the integrity of the personal information in its possession or under its control is secure.

Further that such information is protected against unauthorised or unlawful processing, accidental loss, destruction or damage, alteration or access by having regard to the requirements set forth in law, in industry practice and generally accepted information security practices and procedures will apply to RIH Training Institute.

### 6.7 General Data Protection Regulation (GDPR)

GDPR is EU related Regulation and relates to the personal information of individuals. It doesn't protect businesses. POPIA, however, extends its protections to legal entities, which means that RIH Training Institute is required to protect information collected about companies and corporations as well as the data of individuals.

RIH Training Institute has implemented or plans to implement the same protection to suppliers' or partners' data in addition to its own data.

### 6.8 Request by Data Subjects

Data Subjects have a right in terms of POPIA to request details of the personal information stored and processed by RIH Training Institute. They can furthermore apply for the removal of said personal information by submitting the prescribed form.

If at any time a Data Subject feels that their right of privacy has been infringed, the said Data Subject may lodge a complaint with the Information Regulator - using the prescribed form - providing specific details of the infringement.

# 7. Procedure

*Section 53(1)*

**Procedure to be followed in making a request ito. PAIA**

1. The requester must use the prescribed form to make the request for access to a record. This must be made to the head of the private body. This request must be made to the address, fax number or electronic mail address of the body concerned [s 53(1)].

2. The requester must provide sufficient detail on the request form to enable the head of the private body to identify the record and the requester.

3. The requester must identify the right that is sought to be exercised or to be protected and provide an explanation of why the requested record is required for the exercise or protection of that right [s 53(2)(d)].

4. 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 head of the private body [s 53(2)(f)].

5. A requester who seeks access to a record containing personal information about that requester is not required to pay the request fee. Every other requester, who is not a personal requester, must pay the required request fee. See Annexures hereunder.

6. The fee that the requester must pay to a private body is R50. The requester may lodge an application to the court against the tender or payment of the request fee [s 54(3)(b)].

7. If the request is granted then a further access fee must be paid for the search, reproduction, and preparation and for any time that has exceeded the prescribed hours to search and prepare the record for disclosure [s 54(6)].

**Procedure to be followed in making a request ito. POPIA**

If an individual requests for correction or deletion of personal information or destroying or deletion of record of personal information in terms of section 24(1) of the POPI Act 4 of 2013, it can be done by requisitioning the necessary application form from the Information Officer.

# 8. Prescribed Fees

*Section 51(1)(f)*

Requesters are also required to pay fees for accessing the records of public and private bodies. This fee covers the cost of searching for the record and copying it.

Please refer to Annexure for any additional information or fees.

The fees for accessing records of this private body are prescribed in the Act:

| ACTIVITY | FEE |
|---|---|
| Copy per A4 Page | R1.10 |
| Printing per A4 page | 75 cents |
| Copy on a CD | R70 |
| Transcription of visual images per A4 page | R40 |
| Copy of a visual image | R60 |
| Transcription of an audio recording per A4 page | R20 |
| Copy of an audio recording | R30 |
| Search and preparation of the record for disclosure | R30 per hour or part thereof, excluding the first hour, reasonably required for the search and preparation. |
| Postage fees have to be paid by the requester for the delivery of their records in the case of both public and private bodies. | |

**Exceptions**

If the Information Officer, Deputy Information Officer, or head of the public/private body thinks that the collection and reproduction of documents will take longer than six hours, he/she must inform the requester (by formal notice) that one third of the access fee is payable upfront as a deposit.

If the record is not provided in the form requested, the access fee that is charged to the requester must not exceed the fee that would have been charged if access was granted in the form requested.

However, this rule does not apply when an alternative form is required because information had to be severed from the record.

If the requester cannot read, view or hear the record in the form held by a public body because of a disability, the public body is required to provide the record in a form that is accessible to the requester.

The access fee charged to the requester must not exceed the fee that would have been charged but for the disability.

# Signing and Declaration

The manual is hereby signed by on this _____ day of _____ 20____ at Burgersfort.

_____

Benny Maphanga - +27 71 348 1720

CEO/Director

# Annexure A – Access to Information

Request Form for Access to a Record of a Private Body

## FORM 2

### REQUEST FOR ACCESS TO RECORD

*Section 77C(1)(a) of the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000*

[Regulation 7]

*NOTE:*

*1. Proof of identity must be attached by the requester.*

*2. If requests made on behalf of another person, proof of such authorisation, must be attached to this form.*

**TO:**

| | |
|---|---|
| Information Officer | Benny Maphanga |
| Postal address | 1150, Burgersfort |
| Physical address | No. 3 Bothashoek Road, Mashamotane,, Burgersfort |
| Phone number | +27 71 348 1720 |
| Fax number | |
| E-mail address | richbaminvestment@gmail.com |

*Mark with an "**X**":*

▢ Request is made in my own name ▢ Request is made on behalf of another person

**B. Particulars of person requesting access to the record**

- *The particulars of the person who requests access to the record must be recorded below.*
- *Furnish an address and/or fax number in the Republic of South Africa to which information must be sent.*
- *Proof of identity is required from both the requester and any person or any party acting on behalf of the requester.*
- *The original identity document or such other proof satisfactory to the Chief Executive Officer or Information Officer will need to be presented with this request by the requester or the requester's representative before the request will be processed.*
- *If the request is made on behalf of another person, proof of the capacity in which the request is made, is also to be presented with this request.*

DETAILS OF REQUESTER

| | | |
|---|---|---|
| Full names and surname: | | |
| Identity number: | | |
| Capacity *(if made on behalf of another person)* | | |
| Postal address: | | |
| Street Address: | | |
| E-mail address: | | |
| Contact Numbers: | Tel. (B) | Fax: |
| | Cell: | |

*If a request is made on behalf of another person the requester is obliged to identify him / herself and to provide proof of the mandate under which the request is made, to the satisfaction of the Information Officer.*

## 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: *(of person on whose behalf request is made)* | | |
| Identity number: | | |
| Postal address: | | |
| Street Address: | | |
| E-mail address: | | |
| Contact Numbers: | Tel. (B) | Fax: |
| | Cell: | |

## D. Particulars of record

*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. 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. The requester's attention is drawn to the grounds on which the private body must or may refuse access to a record (in certain instances this may be mandatory, in others it may be discretionary):*

- *Privacy of a third party who is a natural person (human being);*
- *Mandatory protection of certain confidential information of a third party;*
- *Mandatory protection of commercial information of third party;*
- *Mandatory protection of the safety of individuals, and the protection of property;*
- *Mandatory protection of records privileged from production in legal proceedings;*
- *Commercial information of a private body;*
- *Mandatory protection of research information of a third party and a private body.*

**DESCRIPTION OF RECORD OR RELEVANT PART OF THE RECORD:**

| | |
|---|---|
| Reference number (if available) | |
| Description of Record | |
| Any particulars of record | |

*Notes to Particular of record:*

- *Your indication as to the required form of access depends on the form in which the record is available.*
- *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.*
- *The fee payable for access to the record, if any, will be determined partly by the form in which access is requested.*

**TYPE OF RECORD:**
(*Mark the applicable box with an "X"*)

| | |
|---|---|
| Record is in written or printed form | |
| Record comprises virtual images (this includes photographs, slides, video recordings,computer-generated images, sketches, etc) | |
| Record consists of recorded words or information which can be reproduced in sound | |
| Record is held on a computer or in an electronic, or machine-readable form | |

**FORM OF ACCESS:**
(*Mark the applicable box with an "X")*

| | |
|---|---|
| Printed copy of record (including copies of any virtual images, transcriptions and information held on computer or in an electronic or machine-readable form) | |
| Written or printed transcription of virtual images (this includes photographs, slides, video recordings, computer-generated images, sketches, etc) | |
| Transcription of soundtrack (written or printed document) | |
| Copy of record on flash drive (including virtual images and soundtracks) | |
| Copy of record on compact disc drive(including virtual images and soundtracks) | |
| Copy of record saved on cloud storage server | |

**MANNER OF ACCESS:**
(*Mark the applicable box with an "X")*

| | |
|---|---|
| Personal inspection of record at registered address of public/private body (including listening to recorded words, information which can be reproduced in sound, or information held on computer or in an electronic or machine-readable form) | |
| Postal services to postal address | |
| Postal services to street address | |
| Courier service to street address | |
| Facsimile of information in written or printed format (including transcriptions) | |
| E-mail of information (including soundtracks if possible) | |
| Cloud share/file transfer | |
| Preferred language | |
| *(Note that if the record is not available in the language you prefer, access may be granted in the language in which the record is available)* | |

**PARTICULARS OF RIGHT TO BE EXERCISED OR PROTECTED:**
(I*f the provided space is inadequate, please continue on a separate page and attach it to this Form. The requester must sign all the additional pages.)*

| | |
|---|---|
| Indicate which right is to be exercised or protected | |
| Explain why the record requested is required for the exercise or protection of the aforementioned right: | |

**E. Fees**

*a) A request fee must be paid before the request will be considered.*
*b) You will be notified of the amount of the access fee to be paid.*
*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*

| | | |
|---|---|---|
| The requester qualifies for an exemption in payment of fees (mark the appropriate box) | YES | NO |
| Reason | | |
| | | |
| | | |
| | | |
| | | |

**F. Notice**

*You will be notified in writing whether your request has been approved or denied and if approved the costs relating to your request, if any. Please indicate your preferred manner of correspondence:*

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

| **Postal Address** | **Facsimile** | **Electronic Communication (Please specify)** |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

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

.....

SIGNATURE OF REQUESTER / PERSON ON WHOSE BEHALF REQUEST IS MADE
*(sign & print name)*

**FOR OFFICIAL USE**

| | |
|---|---|
| **Reference number:** | |
| **Request received by:** (State Rank, Name And Surname of Information Officer) | |
| **Date received:** | |
| **Access fees:** | |
| **Deposit (if any):** | |

_____

Benny Maphanga

# Annexure B – Fees Schedule

PROMOTION OF ACCESS TO INFORMATION ACT, 2000

REGULATIONS RELATING TO THE PROMOTION OF ACCESS TO INFORMATION

The Minister for Justice and Constitutional Development has, under section 92 of the Promotion of Access to Information Act, 2000 (Act No. 2 of 20001, made the regulations in the Schedule.

SCHEDULE

**Definition**

1. In these Regulations any word or expression to which a meaning has been assigned in the Act shall bear that meaning and, unless the context otherwise indicates -

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

**Form of request**

2. A request for access to a record, as contemplated in section 18(1) of the Act, must be made in the form of Form A of the Annexure.

**Fees for records of public body**

3 (1) The fee for reproduction, referred to in section 15(3:1 of the Act, is as follows:

| | | R |
|---|---|---|
| (a) | For every photocopy of an A4-size page or part thereof | 0.60 |
| (b) | For every printed copy of an A4-size page or part thereof held on a computer or in electronic or machine readable form | 0.40 |
| (c) | For a copy in a computer-readable form on - | |
| | (i) stiffy disc | 5.00 |
| | (ii) compact disc | 40.00 |
| (d) | (i) For a transcription of visual images, for an A4-size page or part thereof | 22.00 |
| | (ii) For a copy of visual images | 60.00 |
| (e) | (i) For a transcription of an audio record, for an A4-size page or part thereof | 12.00 |
| | (ii) For a copy of an audio record | 17.00 |
| (2) | The request fee payable by every requester, other than a personal requester referred to in section 22(1) of the Act, is | 35.00 |
| (3) | The access fees payable by a requester referred to in section 22(7) of the Act, unless exempted under section 22(8) of the Act, are as follows: | |
| (a) | For every photocopy of an A4-size page or part thereof | 6.00 |
| (b) | For every printed copy of an A4-size page or part thereof held on a computer or in electronic or machine readable form | 0.40 |
| (c) | For a copy in a computer-readable form on - | |
| | (i) stiffy disc | 5.00 |
| | (ii) compact disc | 40.00 |
| (d) | (i) For a transcription of visual images, for an A4-size page or part thereof | 22.00 |
| | (ii) For a copy of visual images | 60.00 |
| (e) | (i) For a transcription of an audio record, for an A4-size page or part thereof | 12.00 |
| | (ii) For a copy of an audio record | 17.00 |
| (f) | To search for the record for disclosure, for each hour or part of an hour excluding the first hour reasonably required for such search. | 15.00 |
| (4) | The actual postal fee is payable when a copy of a record must be posted to a requester | |

(5) For purposes of section 22(2) of the Act the following applies:

(a) Six hours as the hours to be exceeded before a deposit is payable; and

(b) one third of the access fee is payable as-a deposit by the requester.

**Form of request**

4. A request for access to a record, as contemplated in section 53(1) of the Act, must be made in the form of Form B of the Annexure.

**Fees for records of private body**

5 (1) The fee for reproduction referred to in section 52i3) of the Act, is as follows:

| | | R |
|---|---|---|
| (a) | For every photocopy of an A4-size page or part thereof | 1.10 |
| (b) | For every printed copy of an A4-size page or part thereof held on a computer or in electronic or machine readable form | 0.75 |
| (c) | For a copy in a computer-readable form on. - | |
| | (i) stiffy disc | 7.50 |
| | (ii) compact disc | 70.00 |
| (d) | (i) For a transcription of visual images, for an A4-size page or part thereof | 40.00 |
| | (ii) For a copy of visual images | 60.00 |
| (e) | (i) For a transcription of an audio record, for an A4-size page or part thereof | 20.00 |
| | (ii) For a copy of an audio record | 30.00 |
| (2) | The request fee payable by a requester, other than a personal requester, referred to in section 54(1) of the Act is | 50.00 |
| (3) | The access fees payable by a requester referred to in section 54(7) of the Act, unless exempted under section 54(8) of the Act, are as follows: | |
| (a) | For every photocopy of an A4-size page or part thereof | 1.10 |
| (b) | For every printed copy of an A4-size page or part thereof held on a computer or in electronic or machine readable form | 0.75 |
| (c) | For a copy in a computer-readable form on - | |
| | (i) stiffy disc | 7.50 |
| | (ii) compact disc | 70.00 |
| (d) | (i) For a transcription of visual images, for an A4-size page or part thereof | 40.00 |
| | (ii) For a copy of visual images | 60.00 |
| (e) | (i) For a transcription of an audio record, for an A4-size page or part thereof | 20.00 |
| | (ii) For a copy of an audio record | 30.00 |
| (f) | To search for the record for disclosure, for each hour or part of an hour reasonably required for such search. | 30.00 |
| (4) | The actual postal fee is payable when a copy of a record must be posted to a requester. | |
| (5) | For purposes of section 54(2) of the Act the following applies: | |
| (a) | Six hours as the hours to be exceeded before a deposit is payable; and | |
| (b) | one third of the access fee is payable as a deposit by the requester. | |

**Notice of internal appeal**

6. Notice of an internal appeal, as contemplated in section 75(1) of the Act, must be lodged in the form of Form C of the Annexure.

**Appeal fees**

7. The appeal fee payable in respect of the lodging of an internal appeal by a requester against the refusal of his or her request for access, as contemplated in section 75(3)( a) of the Act is 50.00 .

**Value -added tax**

8. Public and private bodies registered under the Value-Added Tax Act, 1991 (Act No. 89 of 1991). as vendors may add value added tax to all fees prescribed in terms of these regulations.

**Commencement**

9. These regulations shall come into operation on 9 March 2001.

# Annexure C – POPI

**FORM 1**

**OBJECTION TO THE PROCESSING OF PERSONAL INFORMATION IN TERMS OF SECTION 11(3) OF THE PROTECTION OF PERSONAL INFORMATION ACT NO. 4 OF 2013**

**REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018**

[Regulation 2]

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): | |
| Fax number / 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): | |
| Fax number/ 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

## 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 NO. 4 OF 2013

**REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018**

[Regulation 3]

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.
4. Submit to the current Information Officer of RIH Training Institute-Benny Maphanga(maphanga.ba@gmail.com)

Mark the appropriate box with an "x".

**Request for: (*Please mark appropriate checkbox*)**

- ❏ 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(s) and surname/ registered name of data subject: | |
| Unique Identifier/Identity Number | |
| Residential, postal or business address: | Code ( ) |
| Contact number(s): | |
| Fax number / 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): | |
| Fax number/ E-mail address: | |
| **C** | **INFORMATION TO BE CORRECTED/DELETED/ DESTRUCTED/ DESTROYED** |
| | |
| | |
| | |
| | |
| | |

| | |
|---|---|
| **D** | **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<br>**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.<br>(Please provide detailed reasons for the request) |
| | |
| | |
| | |
| | |

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

.....

Signature of data subject/designated person

## FORM 3

## INFORMATION OFFICER'S REGISTRATION FORM

### IN TERMS OF PROTECTION OF SECTION 55(2) OF THE PERSONAL INFORMATION ACT 4 OF 2013

Note:

1. The personal information submitted herein shall be solely used for your registration with the Information Regulator ("Regulator").
2. All the information submitted herein shall be used for the purpose stated above, as mandated by law. This information may be disclosed to the public.
3. The Regulator undertakes to ensure that appropriate security control measures are implemented to protect all the information to be submitted in this document.
4. A list of all designated Deputy Information Officers must be attached to this Form including their names, official postal and street address, phone, fax number and, electronic mail address
5. A body must, if necessary, update the particulars of an Information Officer and Deputy Information Officer(s) at intervals of not more than one year.
6. This form must be sent to: The Information Regulator, registration.IR@justice.gov.za or P.O Box 31533, Braamfontein, Johannesburg, 2017.

| **A** | **INFORMATION OFFICER** | | |
|---|---|---|---|
| Full Name of Information Officer: | Benny Maphanga | | |
| Designation: | CEO | | |
| Postal Address: | 1150, Burgersfort<br>Code ( ) | | |
| Physical Address: | No. 3 Bothashoek Road, Mashamotane,, Burgersfort<br>Code ( ) | | |
| Cell phone Number: | +27 71 348 1720 | | |
| Landline Number: | +27 71 348 1720 | | |
| Fax number: | | | |
| Direct E-mail address: | maphanga.ba@gmail.com | | |
| General Email address: | richbaminvestment@gmail.com | | |
| **B** | **DEPUTY INFORMATION OFFICER** | | |
| Full Name of Information Officer: | Name: | Name: | Name: |
| | | | |
| | Direct Landline: | Direct Landline | Direct Landline |
| | | | |
| | Cell phone Number: | Cell phone Number: | Cell phone Number: |
| | | | |
| | Email Address: | Email Address: | Email Address: |
| | | | |
| | Site/Department: | Site/Department: | Site/Department: |
| | | | |
| Postal Address: | 1150, Burgersfort<br>Code ( ) | | |

| | | | | |
|---|---|---|---|---|
| Physical Address: | No. 3 Bothashoek Road, Mashamotane,, Burgersfort<br>Code ( ) | | | |
| Fax number: | | | | |
| General Email address: | richbaminvestment@gmail.com | | | |
| **C** | **BODY / RESPONSIBLE PARTY** | | | |
| Type of Body: | Public Body | | Private Body | |
| Full Name of the Body (Registered Name) | Richbam Investment Holdings (Pty) Ltd. | | | |
| Trading Name: | RIH Training Institute | | | |
| Registration No.: | 2018/204169/07 | | | |
| Postal Address: | 1150, Burgersfort<br>Code ( ) | | | |
| Physical Address: | No. 3 Bothashoek Road, Mashamotane,, Burgersfort<br>Code ( ) | | | |
| Landline Number: | +27 71 348 1720 | | | |
| Fax number: | | | | |
| E-mail address: | richbaminvestment@gmail.com | | | |
| Website: | www.rihtraining.co.za | | | |
| **D** | **DECLARATION** | | | |
| | I declare that the information contained herein is true, correct, and accurate. | | | |
| | SIGNED and DATED at _____on this the_____day of _____202___ | | | |
| | _____<br>INFORMATION OFFICER | | | |

**FORM 3 (CONTINUED)**

THE FOLLOWING INFORMATION IS REQUIRED FOR STATISTICAL PURPOSES

| E | STATISTICAL INFORMATION | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **GOVERNMENT** | | | **PUBLIC ENTITIES** | | | **PRIVATE BODIES** | | | **PROFESSION** | | |
| **#** | **Classification of Government** | **X** | **#** | **Classification of Public Entity** | **X** | **#** | **Name of Industry Sector** | **X** | **#** | **Type of Profession** | **X** |
| 1. | National Government | | 1. | Constitutional Entities | | 1. | Education | | 1. | Legal | |
| 2. | Provincial Government | | 2. | Schedule 2 Public Entity | | 2. | Financial | | 2. | Built Environment | |
| 3. | Local Government | | 3. | Schedule 3A Public Entity | | 3. | Health Facilities | | 3. | Financial | |
| | **Legislature** | | 4. | Schedule 3B Public Entity | | 4. | Telecommunications | | 4. | Medical and Allied Health Services | |
| 1. | National Assembly | | 5. | Schedule 3C Public Entity | | 5. | Pharmaceutical | | | **Others, specify** | |
| 2. | National Council of Provinces | | | **Others, specify** | | 6. | Media and Social Media | | 5. | | |
| 3. | Gauteng Provincial Legislature | | | | | 7. | Retail/Direct Marketing | | | | |
| 4. | Western Cape Provincial Legislature | | | | | 8. | Tourism | | | | |
| 5. | Northern Cape Provincial Legislature | | | | | 9. | Transportation, Storage & Logistics | | | | |
| 6. | Limpopo Provincial Legislature | | | | | 10. | Manufacturing/Production | | | | |
| 7. | North West Provincial Legislature | | | | | 11. | Banks | | | | |
| 8. | Free State Provincial Legislature | | | | | 12. | International Organisation | | | | |
| 9. | Mpumalanga Provincial Legislature | | | | | 13. | Real Estate | | | | |
| 10. | Eastern Cape Provincial Legislature | | | | | | **Others, specify** | | | | |
| 11. | Kwazulu Natal Provincial Legislature | | | | | | | | | | |

## FORM 4

## INFORMATION OFFICER'S APPOINTMENT

**REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018**

[Regulation 3&4]

Note:

1. The personal information submitted herein shall be solely used for your registration with the Information Regulator ("Regulator").
2. All the information submitted herein shall be used for the purpose stated above, as mandated by law. This information may be disclosed to the public.
3. Information Officers need to be registered with the Regulator before taking up their duties.
4. A signed copy of this document can be included as an appendix to the designated Information Officer's current employment contract.

**Benny Maphanga,**
CEO of
**Richbam Investment Holdings (Pty) Ltd.**

is hereby appointed as the Information Officer for said Business.

Section 55(1) of POPIA sets out the duties and responsibilities of an Information Officer which include the following:-

1. to encourage compliance with POPI
2. dealing with requests made to the organisation in relation to POPI (for instance, requests from Data Subjects to update or view their personal information)
3. working with the Regulator in relation to investigations
4. otherwise ensuring compliance with POPI
5. as may be prescribed (i.e. keep an eye on the Regulator's website!)

Furthermore, Regulation 4 lists the following prescribed responsibilities in addition to those listed above:

- Compliance framework:
  - develop and implement a compliance framework
  - ensure it is monitored and maintained over time
  - (this could be captured in a privacy charter or framework document that outlines who is responsible for what and which policies apply)
- Personal information impact assessment ("PIIA")
  - conduct a PIIA to ensure that adequate measures and standards exist in order to comply the conditions for the lawful processing of personal information (as defined in Chapter 3 of POPIA)
  - (you can find international guidelines on this if you look up Privacy Impact Assessments or "PIA")
- POPIA Manual: ensure that your organisation has a POPIA manual
  - ensure it is monitored, maintained and made available as prescribed PAIA
  - provide copies of the manual to anyone who asks for it (the Regulator may determine in future that a fee must be paid for this)
- Enable Data Subject Participation
  - develop measures and adequate systems to process requests for information or access to information
  - appoint Deputy Information Officers to assist in these responsibilities
  - provide Business wide training to all employees on the processing of Personal Information,
- Awareness Training: conduct internal awareness sessions regarding:
  - the provisions of the POPI Act,
  - the regulations made in terms of the Act,
  - codes of conduct, or
  - information obtained from the Regulator
  - (this will need to be ongoing as the Regulator provides updates, guidelines, new regulations, or as new codes of conduct become enforceable)

The manual is hereby signed by on this _____ day of _____ 20____
at Burgersfort.

_____

Benny Maphanga - +27 71 348 1720
CEO/Director

## FORM 5

## APPLICATION FORM FOR PRIOR AUTHORISATION

**Guidance Note of the Information Regulator 11 March 2021**

[Section 58(1)]

Note:

1. The personal information submitted herein shall be solely used for purposes of prior authorisation application submitted to the Information Regulator ("Regulator") in terms of section 58(1) of the Protection of Personal Information Act, 2013 (POPIA).
2. All the information submitted herein shall be used for the purpose stated above, as mandated by law. This Information may be disclosed to the public. The Regulator undertakes to ensure that appropriate security control measures are implemented to protect all the personal information to be submitted in this document.

| **A** | **BODY / RESPONSIBLE PARTY** | | | |
|---|---|---|---|---|
| Type of Body: | Public Body | | Private Body | |
| Full Name of the Body (Registered Name) | Richbam Investment Holdings (Pty) Ltd. | | | |
| Trading Name: | RIH Training Institute | | | |
| Registration No.: | 2018/204169/07 | | | |
| Full Name of Information Officer | Benny Maphanga | | | |
| Information Officer's Registration Number | | | | |
| Postal Address: | 1150, Burgersfort<br>Code ( ) | | | |
| Physical Address: | No. 3 Bothashoek Road, Mashamotane,, Burgersfort<br>Code ( ) | | | |
| Landline Number: | +27 71 348 1720 | | | |
| Fax number: | | | | |
| E-mail address: | richbaminvestment@gmail.com | | | |
| Website: | www.rihtraining.co.za | | | |

| B | NOTIFICATION OF PROCESSING - WHICH IS SUBJECT TO PRIOR AUTHORISATION | |
|---|---|---|
| Please select a **category** of personal information you intend to process which is subject to a prior authorisation | | |
| | **Unique identifiers of data subjects for a purpose other than the one for which the identifier was specifically intended at collection; and with the aim of linking the information together with information processed by other responsible parties;** | |
| | Specify nature or categories of Identifiers: | |
| | | |
| | | |
| | **Criminal behaviour or on unlawful or objectionable conduct of data subject on behalf of third parties** | |
| | Specify nature or categories of unlawful or objectionable conduct | |
| | | |
| | | |
| | **Credit reporting** | |
| | **Transfer of the special personal information or personal information of children, to a third party in a foreign country that does not provide an adequate level of protection for the processing of personal information** | |
| | Specify the Country(ies): | |
| | | |
| | **Any other types of information processing by law or regulation which the Regulator has considered that it carries a particular risk for the legitimate interests of the data subject** | |
| | Specify the type(s) of information processing, if any: | |
| | | |
| **Reasons why it is necessary to process the personal information.** | | |
| | | |
| | | |
| **Is the processing of the personal information for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party? If so,specify the function or activity.** | Yes | |
| | | |
| | | |
| | No | |
| | | |
| **Is the function or activity of the responsible party regulated by another regulatory body? If so, specify the regulatory body and proof of registration or authorisation to perform the function must also be provided or attached.** | Yes | |
| | No | |

| | | | | | | |
|---|---|---|---|---|---|---|
| **Please specify the categories of data subjects whose information will be or is being processed.** | Employees/Prospective Employees | | Customers /Prospective Customers or Clients /Prospective Clients | | Children | |
| | Users | | Students | | Vulnerable adults | |
| | Subscribers | | Patients | | Other (Specify) | |
| **Estimated number of data subjects whose processing of their personal information is subject to prior authorisation.** | | | | | | |
| **Security measures to be implemented to ensure the confidentiality, integrity and availability of the information which is to be processed.** | | | | | | |
| | | | | | | |
| | | | | | | |
| **Has the staff member involved in the intended processing of personal information received Personal Information Protection training in the last 2 years? If so, please specify the nature of the training.** | | | | | | |
| **Has the organisation suffered any security breach in the past three (3) months? If so, please specify-<br>a) the nature of the Breach;<br>b) the preventative measures put in place; and<br>c) if the data subjects and<br>the Regulator has been notified about the breach.** | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| **Date on which business activities of the responsible party commenced.** | | | | | | |
| **Number of employees employed by the responsible party** | | | | | | |
| **Number of branches in South African and outside South Africa.** | | | | | | |
| **Number of Deputy Information Officers designated or delegated.** | | | | | | |

| C | DECLARATION |
|---|---|
| | I declare that the information contained herein is true, correct, and accurate. |
| | SIGNED and DATED at _____on this the_____day of _____202___ |
| | _____<br>INFORMATION OFFICER |

**FORM 5 (CONTINUED)**

THE FOLLOWING INFORMATION IS REQUIRED FOR STATISTICAL PURPOSES

| E | STATISTICAL INFORMATION | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **GOVERNMENT** | | | **PUBLIC ENTITIES** | | | **PRIVATE BODIES** | | | **PROFESSION** | | |
| **#** | **Classification of Government** | **X** | **#** | **Classification of Public Entity** | **X** | **#** | **Name of Industry Sector** | **X** | **#** | **Type of Profession** | **X** |
| 1. | National Government | | 1. | Constitutional Entities | | 1. | Education | | 1. | Legal | |
| 2. | Provincial Government | | 2. | Schedule 2 Public Entity | | 2. | Financial | | 2. | Built Environment | |
| 3. | Local Government | | 3. | Schedule 3A Public Entity | | 3. | Health Facilities | | 3. | Financial | |
| | **Legislature** | | 4. | Schedule 3B Public Entity | | 4. | Telecommunications | | 4. | Medical and Allied Health Services | |
| 1. | National Assembly | | 5. | Schedule 3C Public Entity | | 5. | Pharmaceutical | | | **Others, specify** | |
| 2. | National Council of Provinces | | | **Others, specify** | | 6. | Media and Social Media | | 5. | | |
| 3. | Gauteng Provincial Legislature | | | | | 7. | Retail/Direct Marketing | | | | |
| 4. | Western Cape Provincial Legislature | | | | | 8. | Tourism | | | | |
| 5. | Northern Cape Provincial Legislature | | | | | 9. | Transportation, Storage & Logistics | | | | |
| 6. | Limpopo Provincial Legislature | | | | | 10. | Manufacturing/Production | | | | |
| 7. | North West Provincial Legislature | | | | | 11. | Banks | | | | |
| 8. | Free State Provincial Legislature | | | | | 12. | International Organisation | | | | |
| 9. | Mpumalanga Provincial Legislature | | | | | 13. | Real Estate | | | | |
| 10. | Eastern Cape Provincial Legislature | | | | | | **Others, specify** | | | | |
| 11. | Kwazulu Natal Provincial Legislature | | | | | | | | | | |

## FORM 6

## REQUEST FOR PERMISSION TO PROCESS PERSONAL INFORMATION

**Guidance Note of the Information Regulator 11 March 2021**

[Section 58(1)]

Note:

1. The personal information submitted herein shall be solely used for purposes of prior authorisation application submitted to the Information Regulator ("Regulator") in terms of section 58(1) of the Protection of Personal Information Act, 2013 (POPIA).
2. All the information submitted herein shall be used for the purpose stated above, as mandated by law. This Information may be disclosed to the public. The Regulator undertakes to ensure that appropriate security control measures are implemented to protect all the personal information to be submitted in this document.

| **A** | **BODY / RESPONSIBLE PARTY** | | | |
|---|---|---|---|---|
| Type of Body: | Public Body | | Private Body | |
| Full Name of the Body (Registered Name) | Richbam Investment Holdings (Pty) Ltd. | | | |
| Trading Name: | RIH Training Institute | | | |
| Registration No.: | 2018/204169/07 | | | |
| Full Name of Information Officer | Benny Maphanga | | | |
| Information Officer's Registration Number | | | | |
| Postal Address: | 1150, Burgersfort<br>Code ( ) | | | |
| Physical Address: | No. 3 Bothashoek Road, Mashamotane,, Burgersfort<br>Code ( ) | | | |
| Landline Number: | +27 71 348 1720 | | | |
| Fax number: | | | | |
| E-mail address: | richbaminvestment@gmail.com | | | |
| Website: | www.rihtraining.co.za | | | |

# Annexure D – Privacy

**WEBSITE PRIVACY STATEMENT**

## Privacy Policy

### Privacy Statement

Below you will find information concerning visits to and the use of Richbam Investment Holdings (Pty) Ltd. 's website(s). RIH Training Institute Group, its subsidiaries and affiliates („RIH Training Institute"), are sensitive to privacy issues on the Internet and recognises the importance of safeguarding all information we receive from you.

This Privacy Statement applies to Personal Information provided by you and collected by RIH Training Institute through its websites as well as both online and offline services. We will use the provided information in the course of our dealings with you to process requests and orders and to provide a more personalised internet and online experience. RIH Training Institute will ensure that all personal information is treated in accordance with the applicable data privacy legislation's such as the Protection of Personal Information Act (POPIA).

For your information, we have provided this statement explaining our online information practices.

### Collection of your Personal Information

In general, you are able to visit RIH Training Institute's website(s) without revealing who you are or any information about yourself. However, our web servers will collect information (standard information that your browser sends to every website visited) for statistical purposes, such as the number of visits, the pages viewed, which website you came from before clicking into the RIH Training Institute website, the key words used to find our site, your IP-address, the browser type and language, access time, etc. RIH Training Institute uses this information for improving its sites and services.

When visiting a RIH Training Institute site we might ask you to consent to providing personal information, such as your email address, name, telephone number, etc. This information is required in order for us to process and fulfil your requests or order and otherwise provide you with the information and services you may request from us. This information will therefore be kept by us as long as is necessary for us to use your information as described above or to comply with our legal obligations (including the processing of your general request, fraud prevention, anti-money laundering and sanction screening).

For security reasons we also keep the IP-address used when the order is registered. In case of e-commerce transactions, Card holder name information is stored by RIH Training Institute in order to ensure effective handling of any problems regarding charging, cancellations and/or credits. At no time will other credit card information, such as the Primary Account Number, Service Code and Expiration date be stored by RIH Training Institute.

Personal information collected on RIH Training Institute sites and services may, in compliance with applicable laws and regulations, be stored and processed in any country in which RIH Training Institute or its subsidiaries maintain facilities.

Many Internet Browser applications allow for Incognito modes, where you as visitor can anonymously access and traverse any website.

**Security of your Personal Information**

RIH Training Institute has a number of security measures in place to protect your personal information. However, when transmitting personal information over the internet, please bear in mind that no transmission over the internet can ever be guaranteed secure. Therefore, please note that RIH Training Institute cannot guarantee the security of any personal information that you transfer over the internet to us.

**Cookies**

We may also use technologies, such as cookies, to collect information about the pages you view, the links you click and other actions you take on our sites and services.

A cookie is a small text file that is placed on your hard disk by a web page server. Cookies contain information that can later be read by a web server in the domain that issued the cookie to you. Cookies cannot be used to run programs or deliver viruses to your computer.

You have the ability to accept or decline cookies. Most web browsers automatically accept cookies, but you can usually modify your browser setting to decline cookies if preferred.

**Other sites**

RIH Training Institute‘s website may contain links to other sites. Although we try to link only to sites that share our high standards and respect for privacy, we are not in any way responsible for the content of the privacy practices employed by other sites.

**Changes to this Privacy Statement**

This privacy policy may be changed by us at any time. The revised policy will be posted to this page so that you are always aware of the information we collect, how we use it, and under which circumstances we disclose it. We encourage you to periodically review this statement to know how RIH Training Institute is protecting your information.

**Contact**

Questions, comments, and requests regarding this Privacy Policy are welcomed and should be addressed to the Information Officer of RIH Training Institute, Benny Maphanga at maphanga.ba@gmail.com.

Please refer to RIH Training Institute’s PAIA Manual for additional information.

**Revision**

This Privacy Policy was updated/revised on: 12/23/2025 16:48:39.

# Annexure E – Policies

**PROTECTION OF PERSONAL INFORMATION (POPIA) POLICY**

The protection of privacy through providing guiding principles that are intended to be applied to the processing of personal information in a context-sensitive manner.



## 1. INTRODUCTION

The right to privacy is an integral human right recognised and protected in the South African Constitution and in the Protection of Personal Information Act 4 of 2013 ("POPIA").

POPIA aims to promote the protection of privacy through providing guiding principles that are intended to be applied to the processing of personal information in a context-sensitive manner.

Through the provision of quality goods and services, the Business is necessarily involved in the collection, use and disclosure of certain aspects of the personal information of clients, customers, employees, and other stakeholders.

A person's right to privacy entails having control over his or her personal information and being able to conduct his or her affairs relatively free from unwanted intrusions.

Given the importance of privacy, the Business is committed to effectively managing personal information in accordance with POPIA's provisions.

## 2. PURPOSE

This purpose of this policy is to protect the Business from the compliance risks associated with the protection of personal information which includes:

a. Breaches of confidentiality. For instance, the Business could suffer loss in revenue where it is found that the personal information of data subjects has been shared or disclosed inappropriately.

b. Failing to offer choice. For instance, all data subjects should be free to choose how and for what purpose the Business uses information relating to them.

c. Reputational damage. For instance, the organisation could suffer a decline in shareholder value following an adverse event such as a computer hacker deleting the personal information held by the Business.

This policy demonstrates the Business's commitment to protecting the privacy rights of data subjects in the following manner:

a. Through stating desired behaviour and directing compliance with the provisions of POPIA and best practice.

b. By cultivating an organisational culture that recognises privacy as a valuable human right.

c. By developing and implementing internal controls for the purpose of managing the compliance risk associated with the protection of personal information.

d. By creating business practices that will provide reasonable assurance that the rights of data subjects are protected and balanced with the legitimate business needs of the Business.

e. By assigning specific duties and responsibilities to control owners, including the appointment of an Information Officer and where necessary, Deputy Information Officers in order to protect the interests of the Business and data subjects.

f. By raising awareness through training and providing guidance to individuals who process personal information so that they can act confidently and consistently.

## 3. POLICY AND SCOPE

This policy and its guiding principles apply to:

a. the Business's governing body

b. All branches, business units and divisions of the Business

c. All employees and volunteers

d. All contractors, suppliers and other persons acting on behalf of the Business

The policy's guiding principles find application in all situations and must be read in conjunction with POPIA as well as the organisation's PAIA Policy as required by the Promotion of Access to Information Act (Act No 2 of 2000).

The legal duty to comply with POPIA's provisions is activated in any situation where there is:

- A processing of
- personal information
- entered into a record
- by or for a responsible person
- who is domiciled in South Africa.

POPIA does not apply in situations where the processing of personal information:

a. is concluded in the course of purely personal or household activities, or

b. where the personal information has been de-identified.

# 4. DEFINITIONS

### 4.1 Personal Information

Personal information is any information that can be used to reveal a person's identity. Personal information relates to an identifiable, living, natural person, and where applicable, an identifiable, existing juristic person (such as a company), including, but not limited to information concerning:

a. race, gender, sex, pregnancy, marital status, national or ethnic origin, colour, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language and birth of a person;

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

c. any identifying number, symbol, email 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;

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.

### 4.2 Data Subject

This refers to the natural or juristic person to whom personal information relates, such as an individual client, customer or a company that supplies the organisation with products or other goods.

### 4.3 Responsible Party

The responsible party is the entity that needs the personal information for a particular reason and determines the purpose of and means for processing the personal information. In this case, the organisation is the responsible party.

### 4.4 Operator

An operator means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party. For example, a third-party service provider that has contracted with the organisation to shred documents containing personal information. When dealing with an operator, it is considered good practice for a responsible party to include an indemnity clause.

### 4.5 Information Officer

The Information Officer is responsible for ensuring the organisation's compliance with POPIA. Where no Information Officer is appointed, the head of the organisation will be responsible for performing the Information Officer's duties.

Once appointed, the Information Officer must be registered with the South African Information Regulator established under POPIA prior to performing his

or her duties. Deputy Information Officers can also be appointed to assist the Information Officer.

**4.6 Processing**

The act of processing information includes any activity or any set of operations, whether or not by automatic means, concerning personal information and includes:

a. the collection, receipt, recording, organisation, collation, storage, updating or modification,

b. retrieval, alteration, consultation or use;

c. dissemination by means of transmission, distribution or making available in any other form; or

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

**4.7 Record**

Means any recorded information, regardless of form or medium, including:

a. Writing on any material;

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

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

d. Book, map, plan, graph or drawing;

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

**4.8 Filing System**

Means any structured set of personal information, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria.

**4.9 Unique Identifier**

Means any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party.

**4.10 De-Identify**

This means to delete any information that identifies a data subject, or which can be used by a reasonably foreseeable method to identify, or when linked to other information, that identifies the data subject.

**4.11 Re-Identify**

In relation to personal information of a data subject, means to resurrect any information that has been de-identified that identifies the data subject, or can be used or manipulated by a reasonably foreseeable method to identify the data subject.

**4.12 Consent**

Means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.

In contracts and forms, consent for the use of personal information must be expressed in the positive with a check mark or cross and cannot be assumed or defaulted by a signature.

**4.13 Direct Marketing**

Means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of:

a. Promoting or offering to supply, services to the data subject; or

b. Requesting the data subject to make a donation of any kind for any reason.

**4.14 Biometrics**

Means a technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition.

## 5. RIGHTS OF DATA SUBJECTS

Where appropriate, the Business will ensure that its clients and customers are made aware of the rights conferred upon them as data subjects. the Business will ensure that it gives effect to the following seven rights:

**5.1 The right to access Personal Information**

The Business recognises that a data subject has the right to establish whether the Business holds personal information related to him, her or it including the right to request access to that personal information. An example of a "Personal Information Request Form" can be found in the Business's PAIA Manual.

**5.2 The right to have Personal Information corrected or deleted**

The data subject has the right to request, where necessary, that his, her or its personal information must be corrected or deleted where the Business is no longer authorised to retain the personal information.

In such circumstances, the Business will give due consideration to the request and the requirements of POPIA. the Business may cease to use or disclose the data subject's personal information and may, subject to any statutory and contractual record keeping requirements, also approve the destruction of the personal information.

**5.3 The right to object to the processing of Personal Information**

The data subject has the right, on reasonable grounds, to object to the processing of his, her or its personal information.

**5.4 The right to object to Direct Marketing**

The data subject has the right to object to the processing of his, her or its personal information for purposes of direct marketing by means of unsolicited electronic communications.

**5.5 The right to complain to the Information Regulator**

The data subject has the right to submit a complaint to the Information Regulator regarding an alleged infringement of any of the rights protected under POPIA and to institute civil proceedings regarding the alleged non-compliance with the protection of his, her or its personal information.

An example of a "POPI Complaint Form" can be found in the Business's PAIA Manual.

**5.6 The right to be informed**

The data subject has the right to be notified that his, her or its personal information is being collected by the Business. The data subject also has the right to be notified in any situation where the Business has reasonable grounds

to believe that the personal information of the data subject has been accessed or acquired by an unauthorised person.

## 6. GENERAL GUIDING PRINCIPLES

All employees and persons acting on behalf of the Business will at all times be subject to, and act in accordance with, the following guiding principles:

### 6.1 Accountability

Failing to comply with POPIA could potentially damage the Business's reputation or expose the organisation to a civil claim for damages. The protection of personal information is therefore everybody's responsibility.

The Business will ensure that the provisions of POPIA and the guiding principles outlined in this policy are complied with through the encouragement of desired behaviour. However, the Business will take appropriate sanctions, which may include disciplinary action, against those individuals who through their intentional or negligent actions and/or omissions fail to comply with the principles and responsibilities outlined in this policy.

### 6.2 Processing limitation

The Business will ensure that personal information under its control is processed:

a. in a fair, lawful and non-excessive manner, and

b. only with the informed consent of the data subject, and

c. only for a specifically defined purpose.

The Business will inform the data subject of the reasons for collecting his, her or its personal information and obtain written consent prior to processing personal information.

Alternatively, where services or transactions are concluded over the telephone or electronic video feed, the Business will maintain a voice recording of the stated purpose for collecting the personal information followed by the data subject's subsequent consent.

The Business will under no circumstances distribute or share personal information between separate legal entities, associated organisations (such as subsidiary companies) or with any individuals that are not directly involved with facilitating the purpose for which the information was originally collected.

Where applicable, the data subject must be informed of the possibility that their personal information will be shared with other aspects of the organisation's business and be provided with the reasons for doing so.

An example of a "POPIA Notice and Consent Form" can be found under Annexure C.

### 6.3 Purpose specification

All of the Business's business units and operations must be informed by the principle of transparency. the Business will process personal information only for specific, explicitly defined and legitimate reasons. the Business will inform data subjects of these reasons prior to collecting or recording the data subject's personal information.

### 6.4 Further processing limitation

Personal information will not be processed for a secondary purpose unless that processing is compatible with the original purpose. Therefore, where the Business seeks to process personal information it holds for a purpose other than the original purpose for which it was originally collected, and where this secondary purpose is not compatible with the original purpose, the Business will first obtain additional consent from the data subject.

### 6.5 Information quality

The Business will take reasonable steps to ensure that all personal information collected is complete, accurate and not misleading.

The more important it is that the personal information be accurate (for example, the beneficiary details of a life insurance policy are of the utmost importance), the greater the effort the organisation will put into ensuring its accuracy.

Where personal information is collected or received from third parties, the Business will take reasonable steps to confirm that the information is correct by verifying the accuracy of the information directly with the data subject or by way of independent sources.

Since the PAIA Manual should be updated on a yearly basis, it is advised that personal information processed by the Business such as employee information be updated on a yearly basis too.

### 6.6 Open communication

The Business will take reasonable steps to ensure that data subjects are notified (are at all times aware) that their personal information is being collected including the purpose for which it is being collected and processed.

The Business will ensure that it establishes and maintains a "contact us" facility, for instance via its website or through an electronic helpdesk, for data subjects who want to:

a. Enquire whether the organisation holds related personal information, or

b. Request access to related personal information, or

c. Request the organisation to update or correct related personal information, or

d. Make a complaint concerning the processing of personal information.

### 6.7 Security safeguards

The Business will manage the security of its filing system to ensure that personal information is adequately protected. To this end, security controls will be implemented in order to minimise the risk of loss, unauthorised access, disclosure, interference, modification or destruction.

Security measures also need to be applied in a context-sensitive manner. For example, the more sensitive the personal information, such as medical information or bank account details, the greater the security required.

The Business will continuously review its security controls which will include regular testing of protocols and measures put in place to combat cyber-attacks on the organisation's IT network.

The Business will ensure that all paper and electronic records comprising personal information are securely stored and made accessible only to authorised individuals.

All new employees will be required to sign employment contracts containing contractual terms for the use and storage of employee information. Confidentiality clauses will also be included to reduce the risk of unauthorised disclosures of personal information for which the organisation is responsible.

All existing employees will, after the required training/consultation process has been followed, be required to sign an addendum to their employment containing the relevant consent and confidentiality clauses.

The Business's operators and third-party service providers will be required to enter into service level agreements with the organisation where both parties pledge their mutual commitment to POPIA and the lawful processing of any personal information pursuant to the agreement.

An example of "Employee Consent and Confidentiality Clause" for inclusion in the Business's employment contracts can be found under Annexure D.

An example of an "SLA Confidentiality Clause" for inclusion in the Business's service level agreements can be found under Annexure E.

### 6.8 Data Subject participation

A data subject may request the correction or deletion of his, her or its personal information held by the organisation. the Business will ensure that it provides a facility for data subjects who want to request the correction of deletion of their personal information. Where applicable, the organisation will include a link to unsubscribe from any of its electronic newsletters or related marketing activities.

## 7. SPECIFIC DUTIES AND RESPONSIBILITIES

### 7.1 Governing Body/Executive

In terms of the Act, the Business's governing body cannot delegate its accountability and is ultimately answerable for ensuring that the organisation meets its legal obligations in terms of POPIA. The governing body may however delegate some of its responsibilities in terms of POPIA to management or other capable individuals.

The governing body is responsible for ensuring that:

a. the Business appoints an Information Officer, and where necessary, a Deputy Information Officer(s).

b. All persons responsible for the processing of personal information on behalf of the organisation:

- may lead to disciplinary action being taken against them.

- understand that they are contractually obligated to protect the personal information they come into contact with, and are aware that a wilful or negligent breach of this policy's processes and procedures

- are appropriately trained and supervised to do so,

c. Data subjects who want to make enquires about their personal information are made aware of the procedure that needs to be followed should they wish to do so.

d. The scheduling of a periodic POPIA Audit in order to accurately assess and review the ways in which the Business collects, holds, uses, shares, discloses, destroys and processes personal information.

### 7.2 Information Officer

The Business's Information Officer is responsible for:

a. Taking steps to ensure the Business's reasonable compliance with the provision of POPIA.

b. Keeping the governing body updated about the organisation's information responsibilities under POPIA. For instance, in the case of a security breach, the Information Officer must inform and advise the governing body of their obligations pursuant to POPIA.

c. Continually analysing privacy regulations and aligning them with the organisation's personal information processing procedures. This will include reviewing the Business's information protection procedures and related policies.

d. Ensuring that POPIA Audits are scheduled and conducted on a regular basis.

e. Ensuring that the Business makes it convenient for data subjects who want to update their personal information or submit POPIA related complaints to the

organisation. For instance, maintaining a "contact us" facility on the Business's website.

f. Approving any contracts entered into with operators, employees and other third parties which may have an impact on the personal information held by the organisation. This will include overseeing the amendment of the Business's employment contracts and other service level agreements.

g. Encouraging compliance with the conditions required for the lawful processing of personal information.

h. Ensuring that employees and other persons acting on behalf of the Business are fully aware of the risks associated with the processing of personal information and that they remain informed about the Business's security controls.

i. Organising and overseeing the awareness training of employees and other individuals involved in the processing of personal information on behalf of the Business.

j. Addressing employees' POPIA related questions.

k. Addressing all POPIA related requests and complaints made by the Business's data subjects.

l. Working with the Information Regulator in relation to any ongoing investigations. The Information Officers will therefore act as the contact point for the Information Regulator authority on issues relating to the processing of personal information and will consult with the Information Regulator where appropriate, with regard to any other matter.

The Deputy Information Officer(s) will assist the Information Officer in performing his or her duties.

**7.3 Information Technology Manager**

The Business 's IT Manager or Chief Technical Officer is responsible for:

a. Ensuring that the Business's IT infrastructure, filing systems and any other devices used for processing personal information meet acceptable security standards.

b. Ensuring that all electronically held personal information is kept only on designated drives and servers and uploaded only to approved cloud computing services.

c. Ensuring that servers containing personal information are sited in a secure location, away from the general office space.

d. Ensuring that all electronically stored personal information is backed-up and tested on a regular basis.

e. Ensuring that all back-ups containing personal information are protected from unauthorised access, accidental deletion and malicious hacking attempts.

f. Ensuring that personal information being transferred electronically is encrypted.

g. Ensuring that all servers and computers containing personal information are protected by a firewall and the latest security software.

h. Performing regular IT audits to ensure that the security of the organisation's hardware and software systems are functioning properly.

i. Performing regular IT audits to verify whether electronically stored personal information has been accessed or acquired by any unauthorised persons.

j. Performing a proper due diligence review prior to contracting with operators or any other third-party service providers to process personal information on the organisation's behalf. For instance, cloud computing services.

### 7.4 Communications Manager

The Business's Communications Manager/Chief Commercial Officer is responsible for:

a. Approving and maintaining the protection of personal information statements and disclaimers that are displayed on the organisation's website, including those attached to communications such as emails and electronic newsletters.

b. Addressing any personal information protection queries from journalists or media outlets such as newspapers.

c. Where necessary, working with persons acting on behalf of the organisation to ensure that any outsourced marketing initiatives comply with POPIA.

### 7.5 Employees and other persons acting on behalf of the Business

Employees and other persons acting on behalf of the Business will, during the course of the performance of their services, gain access to and become acquainted with the personal information of certain clients, suppliers and other employees.

Employees and other persons acting on behalf of the Business are required to treat personal information as a confidential business asset and to respect the privacy of data subjects.

#### 7.5.1 Processing of Information

Employees and other persons acting on behalf of the Business may not directly or indirectly, utilise, disclose or make public in any manner to any person or third party, either within the Business or externally, any personal information, unless such information is already publicly known, or the disclosure is necessary in order for the employee or person to perform his or her duties.

Employees and other persons acting on behalf of the Business must request assistance from the Information Officer or their line manager if they are unsure about any aspect related to the protection of a data subject's personal information.

Employees and other persons acting on behalf of the Business will only process personal information where:

a. The data subject, or a competent person where the data subject is a child, consents to the processing; or

b. The processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party; or

c. The processing complies with an obligation imposed by law on the responsible party; or

d. The processing protects a legitimate interest of the data subject; or

e. The processing is necessary for pursuing the legitimate interests of the organisation or of a third party to whom the information is supplied.

Furthermore, personal information will only be processed where the data subject:

a. Clearly understands why and for what purpose his, her or its personal information is being collected; and

b. Has granted the organisation with explicit written or verbally recorded consent to process his, her or its personal information.

#### 7.5.2 Consent

Employees and other persons acting on behalf of the Business will consequently, prior to processing any personal information, obtain a specific and informed expression of will from the data subject, in terms of which permission is given for the processing of personal information.

Informed consent is therefore when the data subject clearly understands for what purpose his, her or its personal information is needed and who it will be shared with. Consent can be obtained in written form which includes any appropriate electronic medium that is accurately and readily reducible to printed form. Alternatively, the Business will keep a voice recording of the data subject's consent in instances where transactions are concluded telephonically or via electronic video feed.

Consent to process a data subject's personal information will be obtained directly from the data subject, except where:

a. the personal information has been made public, or

b. where valid consent has been given to a third party, or

c. the information is necessary for effective law enforcement.

Employees and other persons acting on behalf of the Business will under no circumstances:

a. Process or have access to personal information where such processing or access is not a requirement to perform their respective work-related tasks or duties.

b. Save copies of personal information directly to their own private computers, laptops or other mobile devices like tablets or smartphones.

c. All personal information must be accessed and updated from the organisation's central database or a dedicated server.

d. Share personal information informally. In particular, personal information should never be sent by email, as this form of communication is not secure.

e. Where access to personal information is required, this may be requested from the Information Officer or the relevant line manager.

f. Transfer personal information outside of South Africa without the express permission from the Information Officer.

**7.5.3 Responsibilities**

Employees and other persons acting on behalf of the Business are responsible for:

a. Keeping all personal information that they come into contact with secure, by taking sensible precautions and following the guidelines outlined within this policy.

b. Ensuring that personal information is held in as few places as is necessary. No unnecessary additional records, filing systems and data sets should therefore be created.

c. Ensuring that personal information is encrypted prior to sending or sharing the information electronically. The IT Manager will assist employees and where required, other persons acting on behalf of the organisation, with the sending or sharing of personal information to or with authorised external persons.

d. Ensuring that all computers, laptops and devices such as tablets, flash drives and smartphones that store personal information are password protected and never left unattended. Passwords must be changed regularly and may not be shared with unauthorised persons.

e. Ensuring that their computer screens and other devices are switched off or locked when not in use or when away from their desks.

f. Ensuring that, where personal information is stored on removable storage media such as external drives, CDs or DVDs that are kept locked away securely when not being used.

g. Ensuring that, where personal information is stored on paper, that such hard copy records are kept in a secure place where unauthorised people cannot access it. For instance, in a locked drawer of a filing cabinet.

h. Ensuring that where personal information has been printed out, that the paper printouts are not left unattended where unauthorised individuals could see or copy them. For instance, close to the printer.

i. Taking reasonable steps to ensure that personal information is kept accurate and up to date. For instance, confirming a data subject's contact details when the client or customer phones or communicates via email. Where a data subject's information is found to be out of date, authorisation must first be obtained from the Information Officer or the relevant line manager to update the information accordingly.

j. Taking reasonable steps to ensure that personal information is stored only for as long as it is needed or required in terms of the purpose for which it was originally collected. Where personal information is no longer required, authorisation must first be obtained from the Information Officer or the relevant line manager to delete or dispose of the personal information in the appropriate manner.

k. Undergoing POPIA Awareness training from time to time.

Where an employee, or a person acting on behalf of the Business, becomes aware or suspicious of any security breach such as the unauthorised access, interference, modification, destruction or the unsanctioned disclosure of personal information, he or she must immediately report this event or suspicion to the Information Officer or the Deputy Information Officer.

## 8. INFORMATION OFFICERS

The Business will appoint an Information Officer and where necessary, a Deputy Information Officer to assist the Information Officer. The Business's Information Officer is responsible for ensuring compliance with POPIA.

There are no legal requirements under POPIA for the Business to appoint an Information Officer. Appointing an Information Officer is, however, considered to be a good business practice, particularly within larger organisations.

Where no Information Officer is appointed, the head of the Business will assume the role of the Information Officer. Consideration will be given on an annual basis to the re-appointment or replacement of the Information Officer and the re-appointment or replacement of any Deputy Information Officers.

Once appointed, the Business will register the Information Officer with the South African Information Regulator established under POPIA prior to performing his or her duties. An example of an "Information Officer Appointment Letter" can be found under Annexure F.

## 9. POPIA AUDIT

The Business's Information Officer will schedule periodic POPIA Audits. The purpose of a POPIA audit is to:

a. Identify the processes used to collect, record, store, disseminate and destroy personal information.

b. Determine the flow of personal information throughout the Business. For instance, the Business's various business units, divisions, branches and other associated organisations.

c. Redefine the purpose for gathering and processing personal information.

d. Ensure that the processing parameters are still adequately limited.

e. Ensure that new data subjects are made aware of the processing of their personal information.

f. Re-establish the rationale for any further processing where information is received via a third party.

g. Verify the quality and security of personal information.

h. Monitor the extent of compliance with POPIA and this policy.

i. Monitor the effectiveness of internal controls established to manage the organisation's POPI related compliance risk.

In performing the POPIA Audit, Information Officers will liaise with line managers in order to identify areas within the Business's operation that are most vulnerable or susceptible to the unlawful processing of personal information. Information Officers will be permitted direct access to and have demonstrable support from line managers and the organisation's governing body in performing their duties.

## 10. REQUEST TO ACCESS PERSONAL INFORMATION

Data subjects have the right to:

a. Request what personal information the organisation holds about them and why.

b. Request access to their personal information.

c. Be informed how to keep their personal information up to date.

Access to information requests can be made by email, addressed to the Information Officer. The Information Officer will provide the data subject with a "Personal Information Request Form". Once the completed form has been received, the Information Officer will verify the identity of the data subject prior to handing over any personal information. All requests will be processed and considered against the organisation's PAIA Policy. The Information Officer will process all requests within a reasonable time.

## 11. POPIA COMPLAINTS PROCEDURE

Data subjects have the right to complain in instances where any of their rights under POPIA have been infringed upon. the Business takes all complaints very seriously and will address all POPIA related complaints in accordance with the following procedure:

a. POPIA complaints must be submitted to the organisation in writing. Where so required, the Information Officer will provide the data subject with a "POPIA Complaint Form".

b. Where the complaint has been received by any person other than the Information Officer, that person will ensure that the full details of the complaint reach the Information Officer within 1 working day.

c. The Information Officer will provide the complainant with a written acknowledgement of receipt of the complaint within 2 working days.

d. The Information Officer will carefully consider the complaint and address the complainant's concerns in an amicable manner. In considering the complaint, the Information Officer will endeavour to resolve the complaint in a fair manner and in accordance with the principles outlined in POPIA.

e. The Information Officer must also determine whether the complaint relates to an error or breach of confidentiality that has occurred and which may have a wider impact on the organisation's data subjects.

f. Where the Information Officer has reason to believe that the personal information of data subjects has been accessed or acquired by an unauthorised

person, the Information Officer will consult with the organisation's governing body where after the affected data subjects and the Information Regulator will be informed of this breach.

g. The Information Officer will revert to the complainant with a proposed solution with the option of escalating the complaint to the organisation's governing body within 7 working days of receipt of the complaint. In all instances, the organisation will provide reasons for any decisions taken and communicate any anticipated deviation from the specified timelines.

h. The Information Officer's response to the data subject may comprise any of the following:

- A suggested remedy for the complaint,
- A dismissal of the complaint and the reasons as to why it was dismissed,
- An apology (if applicable) and any disciplinary action that has been taken against any employees involved.

i. Where the data subject is not satisfied with the Information Officer's suggested remedies, the data subject has the right to complain to the Information Regulator.

j. The Information Officer will review the complaints process to assess the effectiveness of the procedure on a periodic basis and to improve the procedure where it is found wanting. The reason for any complaints will also be reviewed to ensure the avoidance of occurrences giving rise to POPIA related complaints.

## 12. DISCIPLINARY ACTION

Where a POPIA complaint or a POPIA infringement investigation has been finalised, the Business may recommend any appropriate administrative, legal and/or disciplinary action to be taken against any employee reasonably suspected of being implicated in any non-compliant activity outlined within this policy.

In the case of ignorance or minor negligence, the Business will undertake to provide further awareness training to the employee.

Any gross negligence or the wilful mismanagement of personal information, will be considered a serious form of misconduct for which the Business may summarily dismiss the employee. Disciplinary procedures will commence where there is sufficient evidence to support an employee's gross negligence.

Examples of immediate actions that may be taken subsequent to an investigation include:

a. Recovery of funds and assets in order to limit any prejudice or damages caused.

b. A referral to appropriate law enforcement agencies for criminal investigation.

c. A recommendation to commence with disciplinary action.

## 13. LEGISLATIVE FRAMEWORK

The Business manages its legislative framework within its defined regulatory and legislative framework as defined within its Compliance Risk Management Framework.

## 14. REFERENCES

Compliance files, policies and manuals are maintained by the compliance function. These include:

a. Compliance Risk Management Framework

b. Compliance Manual including all Policies, Processes and Procedures

Requests for any compliance information or documentation to be submitted to Information Officer currently Benny Maphanga at maphanga.ba@gmail.com.

# FORMS

## ANNEXURE C – POPIA NOTICE AND CONSENT FORM

[Business Letterhead]

Dear Employee,

1. We understand that your personal information is important to you and that you may be apprehensive about disclosing it. Your privacy is just as important to us and we are committed to safeguarding and processing your information in a lawful manner.

2. We also want to make sure that you understand how and for what purpose we process your information. If for any reason you think that your information is not processed in a correct manner, or that your information is being used for a purpose other than that for what it was originally intended, you can contact our Information Officer.

3. You can request access to the information we hold about you at any time and if you think that we have outdated information, please request us to update or correct it.

Our Information Officer's Contact Details

| Name | Contact No | Email |
|---|---|---|
| | | |

4. Purpose for Processing your Information

4.1 We collect, hold, use and disclose your personal information mainly to provide you with access to the services and products that we provide. We will only process your information for a purpose you would reasonably expect, including:

[Add/Edit/Delete any purpose that deems applicable]

- Providing you with advice, products and services that suit your needs as requested
- To verify your identity and to conduct credit reference searches
- To issue, administer and manage your insurance policies
- To process insurance claim s and to take recovery action
- To notify you of new products or developments that maybe of interest to you
- To confirm, verify and update your details
- To comply with any legal and regulatory requirements

4.2 Some of your information that we hold may include, your first and last name, email address, a home, postal or other physical address, other contact information, your title, birth date, gender, occupation, qualifications, past employment, residency status, your investments, assets, liabilities, insurance, income, expenditure, family history , medical information and your banking details.

[Add/Edit/Delete any purpose that deems applicable]

5. Consent to Disclose and Share your Information

5.1 We may need to share your information to provide advice, reports, analyses, products or services that you have requested.

5.2 Where we share your information, we will take all precautions to ensure that the third party will treat your information with the same level of protection as required by us. Your information may be hosted on servers managed by a third-party service provider, which may be located outside of South Africa.

5.3 In certain cases we will in any event first require your express consent for further processing of your information.

I hereby authorise and consent to the Business sharing my personal information for purposes mentioned above.

| Name | Date | Signature |
|---|---|---|
| | | |

## ANNEXURE D: EMPLOYEE CONSENT AND CONFIDENTIALITY CLAUSE

**EMPLOYEE CONSENT AND CONFIDENTIALITY CLAUSE**

1. "POPIA" shall mean the Protection of Personal Information Act 4 of 2013 as amended from time to time.

2. The employer undertakes to process the PI of the employee only in accordance with the conditions of lawful processing as set out in terms of POPIA and in terms of the employer's relevant policy available to the employee on request and only to the extent that ii is necessary to discharge its obligations and to perform its functions as an employer and within the framework of the employment relationship and as required by South African law.

3. The employee acknowledges that the collection of his/her PI is both necessary and requisite as a legal obligation, which falls within the scope of execution of the legal functions and obligations of the employer. The employee therefore irrevocably and unconditionally agrees:

o That he/she consents and authorises the employer to undertake the collection, processing and further processing of the employee's PI by the employer for the purposes of securing and further facilitating the employee's employment with the employer.
o Without derogating from the generality of the afore stated, the employee consents to the employer's collection and processing of PI pursuant to any of the employer's Internet, Email, and Interception policies in place insofar as PI of the employee is contained in relevant electronic communications.
o To make available to the employer all necessary PI required by the employer for the purpose of securing and further facilitating the employee's employment with the employer.
o To absolve the employer from any liability in terms of POPIA for failing to obtain the employee's consent or to notify the employee of the reason for the processing of any of the employee's PI.
o To the disclosure of his/her PI by the employer to any third party, where the employer has a legal or contractual duty to disclose such PI.
o The employee further agrees to the disclosure of his/her PI for any reason enabling the employer to carry out or to comply with any business obligation the employer may have or to pursue a legitimate interest of the employer in order for the employer to perform its business on a day-to-day basis.
o The employee authorises the employer to transfer his/her PI outside of the Republic of South Africa for any legitimate business purpose of the employer within the international community. The employer undertakes not to transfer or disclose his/her PI unless it is required for its legitimate business requirements and shall comply strictly with legislative stipulations in this regard.

4. The employee acknowledges that during the course of the performance of his/her services, he/she may gain access to and become acquainted with the personal information of certain clients, suppliers and other employees. The employee will treat personal information as a confidential business asset and agrees to respect the privacy of clients, suppliers and other employees.

5. To the extent that he/she is exposed to or insofar as PI of other employees or third parties are disclosed to him/her, the employee hereby agree to be bound by appropriate and legally binding confidentiality and non-usage obligations in relation to the PI of third parties or employees.

6. Employees may not directly or indirectly, utilise, disclose or make public in any manner to any person or third party, either within the organisation or externally, any personal information, unless such information is already publicly known, or the disclosure is necessary in order for the employee or person to perform his or her duties on behalf of the employer.

| Name | Date | Signature |
|---|---|---|
| | | |

# ANNEXURE E: SLA CONFIDENTIALITY CLAUSE

## SERVICE LEVEL AGREEMENT - CONFIDENTIALITY

Agreement between

**Richbam Investment Holdings (Pty) Ltd.**

Hereafter referred to as “the Business’

and

_____

Hereafter referred to as “Service Provider”

1. Definitions

"Personal Information" shall mean:

- the race, gender, sex, pregnancy, marital status, national or ethnic origin, colour, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language and birth of a person;
- information relating to the education or the medical, financial, criminal or employment history of the person;
- any identifying number, symbol, email address, physical address, telephone number, location information, on-line identifier or other particular assignment to the person;
- the biometric information of the person;
- the personal opinions, views or preferences of the person;
- 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;
- the views or opinions of another individual about the person whether the information is recorded electronically or otherwise.

"POPIA" shall mean the Protection of Personal Information Act 4 of 2013 as amended from time to time.

2. The parties acknowledge that for the purposes of this agreement that the parties may come into contact with or have access to PI and other information that may be classified or deemed as private or confidential and for which the other party is responsible.

3. Such Personal Information may also be deemed or considered as private and confidential as it relates to any third party who may be directly or indirectly associated with this agreement. Further, ii is acknowledged and agreed by the parties that they have the necessary consent to share or disclose the PI and that the information may have value.

4. The parties agree that they will at all times comply with POPIA's Regulations and Codes of Conduct and that it shall only collect, use and process Personal Information it comes into contact with pursuant to this agreement in a lawful manner, and only to the extend required to execute the services, or to provide the goods and to perform their respective obligations in terms of this agreement.

5. The parties agree that it shall put in place, and at all times maintain, appropriate physical, technological and contractual security measures to ensure the protection and confidentiality of PI that ii, or its employees, its contractors or other authorised individuals comes into contact with pursuant to this agreement.

6. Unless so required by law, the parties agree that it shall not disclose any Personal Information as defined in POPIA to any third party without the prior written consent of the other party, and notwithstanding anything to the contrary contained herein, shall any party in no manner whatsoever transfer any PI out of the Republic of South Africa.

For the Business

| Name | Date | Signature |
|---|---|---|
| | | |

For the Service Provider

| Name | Date | Signature |
|---|---|---|
| | | |

## STAFF CONFIRMATION SHEET

I confirm that I have read and understand the contents of this document and that I am aware of my duties in respect thereof

| Name | Date | Signature |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |