

Troudees (Pty) Ltd.

Protection of Personal Information Code of Conduct  
(POPI)

2021



Prepared by: Compliance Department

Date: 01 June 2021

DOCUMENT DETAILS	
Document title	Trouldees (Pty) Ltd. POPI Code of Conduct
Document owner	Trouldees (Pty) Ltd.
Document classification	General
Document category	Policy
Version number	TI POPI001
Approved date	01 June 2021
Implementation date	01 July 2021
Next review date	31 May 2022

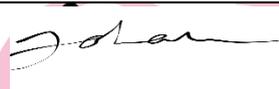
Approvals			
Approval	Name	Signature	Date
Prepared by:	Compliance Officer		30/06/2021
Approved by:	Managing Director		

Table of Contents

1. Purpose..... 4

2. Application ..... 4

3. Background..... 4

4. Protection Of Personal Information Act, Act 4 Of 2013 ..... 4

5. Information Officer ..... 4

6. Duties Of Information Officer ..... 6

7. Deputy Information Officer ..... 8

8. Duties Of Deputy Information Officer ..... 9

9. Notification Of Security Compromises ..... 9

9.1. To The Data Subject..... 9

9.2. To The Information Regulator ..... 10

9.3. By Information Officer ..... 10

9.4. By Deputy Information Officer..... 10

9.5. By Employees ..... 10

10. Training ..... 10

11. Section 5 Notice..... 10

12. Eight Conditions..... 11

12.1. Accountability ..... 11

12.2. Processing Limitation ..... 11

12.3. Purpose Specification ..... 11

12.4. Further Processing Limitation ..... 11

12.5. Information Quality..... 12

12.6. Openness..... 12

12.7. Security Safeguards ..... 12

12.8. Data Subject Participation ..... 12

13. Company POPI Policy ..... 13

14. Employer Obligation ..... 13

15. Employee Obligation..... 13

16. Learner Obligation ..... 13

17. Third-Party Obligation..... 13

18. Internal Audit..... 14

19. Non-Adherence to POPI Code of Conduct ..... 14

20. Non-Adherence to Company POPI Act Policy..... 14

21. Company Code of Conduct ..... 14



## 1. Purpose

This code of conduct aims to create and implement certain guidelines and safeguard measures as required by the Protection of Personal Information Act, Act 4 of 2013 ("POPI"), in an attempt to comply with the regulations of the POPI Act.

## 2. Application

This Code of Conduct applies to any Trouldees (Pty) Ltd. employee, sub-contractor and/or any third party acting on behalf of Trouldees (Pty) Ltd.

## 3. Background

This Code of Conduct is drafted and implemented as a compulsory requirement in terms of the POPI act. As of 1 July 2021, all South African institutions, both in the public and private sectors are obligated to be fully compliant with the requirements placed on them by the POPI Act. This obligation then serves as the background for the drafting and implementation of this code of conduct.

## 4. Protection Of Personal Information Act, Act 4 Of 2013

The Protection of Personal Information Act, Act 8 of 2013 ("POPIA"), regulates the gathering, disposal of, storage and sharing of personal information in South Africa. As of 01 July 2021, all South African Institutions, in both the public and private sectors are obligated to comply with the relevant sections of the POPI act. Therefore, this code of conduct is implemented not only as a requirement of the POPI Act but as a guideline and on how Trouldees (Pty) Ltd. will be compliant with the POPI Act.

## 5. Information Officer

Information Officers ("IO") are, by their position, appointed automatically in terms of the Promotion of Access to Information Act ("PAIA") and POPIA.

Trouldees (Pty) Ltd. is a private body therefore the IO for Trouldees (Pty) Ltd. will be any person holding the position of Managing Director. In terms of PAIA and POPIA, an IO is allowed to delegate the IO's authority to any natural person who is an employee of such public or private body.

The following are categories of IO per specific body. For this Code of Conduct, the IO of a private body will be applicable.

Nature of the Body	Identity of Information Officer	
<b>Public Body, Department or Organ of State</b> (as defined in Section 239 of the Constitution)	National Department of Provincial Government Components.	Director-General or the person who is acting as such.
	Presidency or a National Government Component.	Director-General or the person who is acting as such.
	Provincial Department or a Provincial Government Component.	Head of Department or the person who is acting as such.
	Office of a Premier or a Provincial Government Component.	Director-General or the person who is acting as such.
	Municipality	Municipal Manager or the person who is acting as such.
	Public Institutions	Chief Executive Officer or the person who is acting as such.
<b>Private Body</b>	Natural Person	A natural person who carries on any trade, business or profession, but only in such capacity or any person duly authorized by that natural person.
	Partnership	Any partner of the partnership or any person duly authorized by the partnership.
	Juristic Person	Chief Executive Officer or the Managing Director or equivalent officer of the juristic person or any person duly authorized by that officer or any person who is.

## 6. Duties Of Information Officer

6.1. Section 55 of the POPIA sets out the duties of Information Officers, which include the following: - the encouragement of compliance by the Body with the conditions for the lawful processing of personal information. For example: -

6.1.1.1 *an Information Officer may develop a policy on how employees should implement the eight (8) conditions for the lawful processing of personal information or consider issuing a circular in the case of provincial and national departments;*

6.1.2 dealing with requests made to the Body according to POPIA. For example: -

6.1.2.1 *an Information Officer of a Body will be expected to render such reasonable assistance, free of charge, as is necessary to enable the requester or data subject to comply with the prescribed process for submitting a request in terms of section 18 of PAIA and section 24 of POPIA. If a requester or data subject has made any request that does not comply with the requirements of PAIA or POPIA, the Information Officer concerned may not refuse the request because of that non-compliance, unless the Information Officer has: -*

- a) *notified the data subject or requester of his/her intention to refuse the request and stated in the notice, the reasons for the contemplated refusal, as well as his/her availability to assist that requester or data subject to remove the grounds for refusal;*
- b) *given the requester or data subject a reasonable opportunity to seek such assistance;*
- c) *as far as reasonably possible, furnished the requester or data subject with any information that would assist the making of the request in the prescribed form; and*
- d) *given the requester a reasonable opportunity to confirm the request or to alter it to comply with section 18 of PAIA or 24 of POPIA.*

6.1.3 working with the Regulator concerning investigations conducted to Chapter 6 of POPIA with the body. For example: -

6.1.3.1 *the responsible party must obtain prior authorisation from the Regulator on the following: -*

- a) *processing of any unique identifiers of data subjects: -*
  - i. *for a purpose other than the one for which the identifier was specifically intended at the collection; and*
  - ii. *to link the information together within information processed by other responsible parties;*
- b) *processing of information on criminal behaviour or unlawful objectionable conduct on behalf of third parties;*
- c) *processing of information for credit reporting; and*

d) *transfer of special personal information or the personal information of children to the third party in a foreign country that does not provide an adequate level of protection for the processing of personal information as referred to in section 72*

6.1.3.2 *pending the authorisation or completion of investigation by the Regulator, or until such time the responsible party receives a notice that a more detailed investigation will not be conducted, the responsible party is prohibited from carrying out information processing. This means that processing that falls under paragraph*

6.1.3.3 *above is suspended pending the authorisation from the Regulator.*

6.1.3.4 *failure to notify the Regulator of the processing listed above is an offence and upon conviction, the responsible party will be liable to a fine or imprisonment for a period not exceeding 12 months, or to both a fine and such imprisonment*

6.1.4 otherwise ensuring compliance by a body with the provisions of POPIA. For example: -

6.1.4.1 *POPIA prescribes eight (8) conditions for the lawful processing of personal information by or for a responsible party and it is the responsibility of an Information Officer to ensure compliance with those conditions.*

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

6.2.1.1. a compliance framework is developed, implemented, monitored and maintained;

6.2.1.2. a personal information impact assessment is done to ensure that adequate measures and standards exist to comply with the conditions for the lawful processing of personal information

6.2.1.3. a manual is developed, monitored, maintained and made available as prescribed in sections 14 and 31 of PAIA, as amended;

6.2.1.4. internal measures are developed together with adequate systems to process requests for information or access thereto;

6.2.1.5. internal awareness sessions are conducted regarding the provisions of POPIA, regulations made in terms of POPIA, codes of conduct, or information obtained from the Regulator; and

6.2.1.6. upon request by any person, copies of the manual are provided to that person upon the payment of a fee to be determined by the Regulator from time to time<sup>13</sup>.

6.3. The Information Officer of each public Body must annually, and in terms of section 32 of PAIA, submit to the Regulator a report regarding-

- 6.3.1. the number of requests for access received;
- 6.3.2. the number of requests for access granted in full;
- 6.3.3. the number of requests for access granted in terms of section 46 of PAIA;
- 6.3.4. the number of requests for access refused in full and refused partially and the number of times each provision of PAIA was relied on to refuse access in full or partially;
- 6.3.5. the number of cases in which the periods stipulated in section 25(1) of PAIA was extended in terms of section 26 (1) of PAIA;
- 6.3.6. the number of internal appeals lodged with the relevant authority and the number of cases in which, as a result of an internal appeal, access was given to a record;
- 6.3.7. the number of internal appeals which were lodged on the ground that a request for access was regarded as having been refused in terms of section 27 of PAIA;
- 6.3.8. the number of applications to a court that were lodged on the ground that an internal appeal was regarded as having been dismissed in terms of section 77 (7) of PAIA.

6.4. The Regulator may, annually, request an Information Officer of a private body, in terms of section 83 (4) of PAIA, to furnish to the Regulator with information about requests for access to records of that body.

6.4.1.1. In the case of health records, if the Information Officer believes that the disclosure of the record to the relevant person would be likely to cause serious harm to their physical or mental health or well-being, the Information Officer may only give access to the record if the requester proves to the satisfaction of the information officer that adequate provision is made for such counselling or arrangements as are reasonably practicable before, during or after the disclosure of the record to limit, alleviate or avoid such harm to the relevant person.

6.5. Registration of Information Officers<sup>15</sup> with the Regulator is not only the prerequisite for an Information Officer to take up their duties in terms of POPIA, but is a compulsory requirement for every person identified in paragraph 5.1 above.

6.6. The Information Officers of public bodies and heads of private bodies under PAIA will register to perform their duties and responsibilities in terms of POPIA.

6.7. The responsible party has to ensure that the Information Officer is registered with the Information Officer.

## 7. Deputy Information Officer

- 7.1. Section 17 of PAIA provides for the designation of a Deputy Information Officer of a public body, and section 56 of POPIA extends the designation of a Deputy Information Officer for a private body.
- 7.2. Only employee(s) of a body can be designated as a Deputy Information Officer.
- 7.3. To render a body as accessible as reasonably possible the Information Officers of public and private bodies must designate one or more Deputy Information Officers as are necessary, depending on the structure and size of such bodies;
- 7.4. More than one (1) Deputy Information Officer can be designated, depending on the size, structure and the complexity of the operations of a specific body;

- 7.5. The decision of whether or not to designate a Deputy Information Officer will depend on the size and structure of a body.
- 7.6. To ensure accessibility, the Information Officer of a multinational entity based outside of the Republic must designate any person within the Republic of South Africa as a Deputy Information Officer.
- 7.7. A designation to a Deputy Information Officer must be in writing;
- 7.8. A person designated as a Deputy Information Officer should be afforded sufficient time, adequate resources and the financial means to devote to matters concerning POPIA and PAIA;
- 7.9. It is recommended that a Deputy Information Officer should report to the highest management office within a Body. This means that only an employee at a level of management and above should ideally be considered for designation as a Deputy Information Officer of a body;
- 7.10. A Deputy Information Officer should be accessible to everyone, particularly to a data subject in respect of POPIA or a requester, in terms of PAIA;
- 7.11. A Deputy Information Officer should have a reasonable understanding of POPIA and PAIA to execute his or her duties.
- 7.12. A Deputy Information Officer should have a reasonable understanding of the business and processes of a body. An employee(s) with institutional knowledge is preferred for designation as a Deputy Information Officer(s).
- 7.13. To ensure accessibility, the designated Deputy Information Officer(s) of a multinational entity must be based within the Republic.

## 8. Duties Of Deputy Information Officer

A Deputy Information Officer will have the same duties as the Information Officer as the authority to act on behalf of the Information Officer have been delegated in writing to the Deputy Information Officer. It is important to note that the Information Officer remains ultimately responsible for compliance with both PAIA and POPIA.

## 9. Notification Of Security Compromises

Section 22 of POPIA places an obligation on a body to notify the data subject of any security compromises the body might have or did suffer, regardless of whether the data subject has been affected or not.

### 9.1. To The Data Subject

Notice of a security compromise must be made to the relevant data subject(s) in writing as soon as possible after the private or public body became aware of the security compromise.

## 9.2. To The Information Regulator

The IO must inform the data subject(s) and the Information Regulator, in writing, as soon as the IO have become aware of the security compromise, of any security compromise/s that had or may have occurred.

## 9.3. By Information Officer

Any security compromise can only be reported to the data subject(s) and the Information Regulator by the appointed Information Officer of Trouldees (Pty) Ltd.

## 9.4. By Deputy Information Officer

The Deputy Information Officer may only report any security compromise to a data subject, or data subjects and the Information Regulator upon the instruction given by the Information Officer to report such security compromise to the Information Regulator on behalf of the Information Officer of Trouldees (Pty) Ltd.

The Deputy Information Officer must report, in writing, any security compromise reported to the Deputy Information Officer by an employee or data subject to the Information Officer as soon as the Deputy Information Officer has received notice of such security compromise.

## 9.5. By Employees

If an employee becomes aware of a security compromise or caused a security compromise, whether intentionally or accidentally, is obligated to report such security compromise, in writing, to the Deputy, or Information Officer, as soon as the employee becomes aware of the security compromise.

## 10. Training

Each employee of Trouldees (Pty) Ltd. including the IO, will be obliged to undergo compulsory POPI Act training both upon commencement of duties and continuously during the employees' employment with Trouldees (Pty) Ltd. It remains the duty of the IO to ensure that said training is scheduled and conducted.

## 11. Section 5 Notice

Personal information of a data subject (individual and/or a juristic person) can and must be gathered for a specific purpose, which purpose must be disclosed to the data subject requested to provide his/her personal information.

Section 5 notice explains to the data subject the data subjects' rights in terms of the POPI Act, such as the purpose the personal information is gathered for, the reason why it gathered, how the personal information will be dealt with and how the personal information will be safeguarded.

The section 5 notice is to be signed by any person including employees, learners, contractors, sub-contractors and or any other third party. This notice explains the data subjects' rights. The signing of the notice by the employee, learner, contractor, subcontractor and or any third party is an acknowledgement by the person signing the notice confirming the data subject read and understood the contents of the notice. No personal information may be gathered from any person or entity without a signed Section 5 Notice.

## 12. Eight Conditions

The POPI Act contains **8 (eight)** conditions on the processing of personal information. These 8 (eight) conditions are the guideline as to how personal information can or is to be handled. Any non – compliance with these eight conditions will result in the breach of POPIA and can or may result in.

### 12.1. Accountability

In terms of Section 8 of POPIA, any public and private body must ensure that all relevant processes and procedures are in place to ensure full compliance with the eight conditions. Trouldees (Pty) Ltd. has appointed an Information Officer as required by PAIA and POPIA who will be the accountable person ensuring full compliance with POPIA.

### 12.2. Processing Limitation

Any personal information obtained from a data subject must be done so lawfully and in a reasonable manner that does not infringe on the data subjects right to privacy. As such Trouldees (Pty) Ltd. binds itself to the lawful and reasonable obtainment of personal information from data subjects.

Trouldees (Pty) Ltd. will never request a data subject to provide personal information that is excessive or more than needed to give effect to the purpose for which the personal information is obtained. Trouldees (Pty) Ltd. will achieve this by requesting the minimal personal information required to perform any contractual obligation we might have. Any personal information obtained that is deemed excessive for the purpose requested will be discarded as per the relevant sections of POPIA.

Any personal information collected by Trouldees (Pty) Lt. will only be collected with the consent of the data subject. Further to this we will at all times ensure that the collection of the personal information will be justified and in line with our objectives.

When and where ever possible any personal information collected by Trouldees (Pty) Ltd. will be collected directly from the data subject.

### 12.3. Purpose Specification

Trouldees (Pty) Ltd. will at all times collect personal information from data subjects for a specific purpose linked to our objectives. The purpose for which personal information is collected by us will be made known and clear to the data subject in our Section 5 Notice.

Personal information collected by Trouldees (Pty) Ltd. will not be stored for any period longer than legally required. The majority of personal information we collect is for Seta purposes and in terms of Seta regulations and accreditation requirements, all records related to Seta must be kept for a minimum period of 3 (three) years. Therefore, any personal information collected from a data subject will be destroyed or discarded 3 (three) after the date of collection.

### 12.4. Further Processing Limitation

Any personal information collected has been collected for a specific purpose and to achieve a certain objective. If we need to further process the personal information collected, we will ensure that any such further processing is compatible with the initial purpose for which the personal information has been gathered.

## 12.5. Information Quality

We will at all times ensure that the information provided to us by a data subject, are correct, not misleading and updated to the most recent personal information. The provision of false, misleading and/or personal information of another data subject is a criminal offence and will result in legal action instituted against the data subject that provided the false, misleading and/or incorrect information of another data subject.

## 12.6. Openness

Trouldees (Pty) Ltd. will make available a manual containing the contact particulars of the IO, Deputy IO and any other person who have been authorised by the IO to act in the IO's stead on the company website.

Trouldees (Pty) Ltd. will at all times notify a data subject when we collect personal information of the relevant data subject.

## 12.7. Security Safeguards

We have implemented organisation-wide safeguard measures to ensure the integrity and confidentiality of any personal information collected by us. This is done by implementing by taking appropriate, reasonable technological and organisational measures. These measures have been implemented in line with our objectives and purpose for which we collect personal information.

Any person collecting personal information on behalf of Trouldees (Pty) Ltd. will be authorised to collect said personal information. Any such person has been trained and educated on the eight conditions regarding the lawful processing of personal information. No unauthorised person is allowed to collect personal information on behalf of Trouldees (Pty) Ltd. An authorised person is not allowed to collect personal information for any other purpose than the purpose for which Trouldees (Pty) Ltd. is collecting personal information, nor is an authorised person allowed to request an unauthorised person to collect personal information on behalf of Trouldees (Pty) Ltd. Any such actions will result in disciplinary action being instituted against such person.

If Trouldees (Pty) Ltd. will have to rely upon or make use of an operator to collect or process personal information on our behalf, such operator will be required to enter into an agreement with us whereby the operator acknowledges and accepts to process any personal information collected on our behalf will be done so in accordance to the eight conditions of POPIA and our internal safeguard measures. Any such non – adherence will result in the termination of the agreement.

Trouldees (Pty) Ltd. not only have a statutory obligation to notify a data subject of a security compromise, but an institutional and corporate governance obligation to inform a data subject of a security compromise. Therefore, we have implemented certain reporting structures to ensure that we adhere to the above obligations placed on us.

## 12.8. Data Subject Participation

A data subject has the right to request from a responsible party whether such responsible party has personal information of the data subject in its possession, and if so, request to provide the data subject with the information on its database.

If any of the personal information provided to the data subject is subject to change, the data subject has the right to request the correction of any incorrect information.

Any request made by a data subject is to be made by submitting the applicable request form, found on our website under "forms" and must be submitted to the email address given on the request form. Any request form not submitted to the given email address will result in not being attended to.

### 13. Company Popi Policy

Trouldees (Pty) Ltd. implemented an internal POPI Act policy to which all employees, learners, contractors, sub-contractors and/or any third party must adhere. This Code of Conduct must be read in conjunction with the said POPI Act policy. The Trouldees (Pty) Ltd. POPI Code of Conduct will also apply to all employees, learners, contractors, sub-contractors and/or any other third party with whom Trouldees (Pty) Ltd. engages.

### 14. Employer Obligation

It is the employer, Trouldees (Pty) Ltd. obligation towards its employees to ensure full compliance with POPIA. To act in the best interest of the company and its employees at all times when dealing with personal information and to ensure that the necessary safeguard measures are in place to ensure the safety of all employees' personal information.

### 15. Employee Obligation

All employees of Trouldees (Pty) Ltd. have an obligation, for the duration of their employment, towards the employer to at all times act within the ambits of this Code of Conduct and POPIA when dealing with personal information.

All employees are further obligated to report any non – adherence to this Code of Conduct or any other POPIA document of the company as soon as the employee became aware of the non – adherence.

### 16. Learner Obligation

Any learner, whether current or prospective, has a legal obligation to provide Trouldees (Pty) Ltd. with correct and truthful personal information of the learner upon request. Any learner who provides false and/or misleading personal information of the learner or any other person will be subjected to criminal prosecution.

All learners are obligated to adhere to the company POPI Policy and POPI Code of Conduct for the duration of their training with Trouldees (Pty) Ltd.

If a learner has become aware of a security compromise, such security compromise must be reported as soon as the learner has become aware of the security compromise.

### 17. Third-Party Obligation

Any third party who engages with Trouldees (Pty) Ltd. or its affiliates are legally obligated to adhere to this Code of Conduct and any other Trouldees (Pty) Ltd.

POPI policies, for the duration of the third party's engagement with Trouldees (Pty) Ltd. Any non – compliance with this Code of Conduct or any other POPI policies will result in the termination of the engagement with the said third party and may be subjected to further legal action to protect the interests of Trouldees (Pty) Ltd.

18. Internal Audit

Trouldees (Pty) Ltd. have implemented internal audit procedures and processes to conduct monthly internal audits to ensure compliance with this Code of Conduct and other POPI policy implemented by Trouldees (Pty) Ltd.

19. Non-Adherence to Popi Code of Conduct

Any non – adherence to the POPI Code of Conduct, whether intentional or accidental can or may result in disciplinary action being instituted.

20. Non-Adherence to Company Popi Act Policy

Any non – adherence to the company POPI Act policy, whether intentional or accidental can or may result in disciplinary action being instituted.

21. Company Code of Conduct

The POPI Act Code of Conduct is further governed by the company code of conduct. As a result, any non – adherence to the POPI Code of Conduct will result in automatic non – adherence to the company Code of Conduct and can and may disciplinary action be instituted as a result of any non – adherence.

The logo for Trouldees features the word "TROULDEES" in a light pink, serif, all-caps font. Overlaid on this is the word "troudees" in a black, lowercase, cursive script font. The script font is positioned such that it appears to be written over the pink text, with the 'i' and 'd' being particularly prominent.

**ANNEXURE A**

**INFORMATION OFFICER'S REGISTRATION FORM**

**NOTE: THE PERSONAL INFORMATION USED IN THIS FORM, SHALL SOLELY BE USED FOR REGISTRATION WITH THE INFORMATION REGULATOR ("REGULATOR")**

All the information supplied in this document 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 the appropriate security control measures are implemented to protect all the information to be submitted in this document.

<b>PART A INFORMATION OFFICER</b>	
<b>FULL NAME</b>	
<b>DESIGNATION</b>	
<b>POSTAL ADDRESS</b>	
<b>PHYSICAL ADDRESS</b>	
<b>CELL PHONE NUMBER</b>	
<b>DIRECT EMAIL ADDRESS</b>	
<b>GENERAL EMAIL ADDRESS</b>	
<b>LANDLINE</b>	

<b>PART B DEPUTY INFORMATION OFFICER</b>		
<b>PERSONAL DETAILS OF DESIGNATED OR DELEGATED DEPUTY OFFICERS</b>	<b>FULL NAME</b>	<b>FULL NAME</b>
	<i>idew</i>	<i>idew</i>
	<b>EMAIL ADDRESS</b>	<b>EMAIL ADDRESS</b>
	<b>DIRECT LANDLINE</b>	<b>DIRECT LANDLINE</b>
	<b>CELL PHONE NUMBER</b>	<b>CELL PHONE NUMBER</b>
<b>POSTAL ADDRESS</b>		
<b>PHYSICAL ADDRESS</b>		
<b>LANDLINE NUMBER</b>		
<b>GENERAL CONTACT EMAIL</b>		

PART C RESPONSIBLY BODY/PARTY			
TYPE OF BODY	PUBLIC COPY		PRIVATE BODY
REGISTERED NAME OF THE BODY			
TRADING NAME			
REGISTRATION NUMBER			
POSTAL ADDRESS			
PHYSICAL ADDRESS			
LANDLINE NUMBER			
GENERAL CONTACT EMAIL ADDRESS			
WEBSITE			

**PART D  
DECLARATION**

I, the undersigned hereby declare that the information provided above are true, correct and accurate.

Signed and dated at \_\_\_\_\_ on this day \_\_\_\_\_ of \_\_\_\_\_ 2021.

*idees*

\_\_\_\_\_  
INFORMATION OFFICER

**ANNEXURE B**

**DESIGNATION AND DELEGATION OF AUTHORITY  
TO THE DEPUTY INFORMATION OFFICER**

(In terms of Section 56 of the Protection of Personal Information Act, 2013 (POPIA)  
and Section 17(1) of the Promotion of Access to Information Act, 200 (PAIA))

I, the undersigned

\_\_\_\_\_  
Information Officer

Hereby designate \_\_\_\_\_ as Deputy Information Officer of \_\_\_\_\_.

Furthermore, I hereby delegate the following powers, duties and responsibilities as imposed on me by POPIA and PAIA; -

a)

Please be advised that I reserve the right to exercise any of the power, duties and responsibilities conferred herein, as well as the right to amend/withdraw any of those duties, power and responsibilities.

\_\_\_\_\_  
INFORMATION OFFICER

By my signature I hereby accept the designation and delegation of Deputy Information Officer.

\_\_\_\_\_  
DEPUTY INFORMATION OFFICER

DATE: \_\_\_\_\_

**ANNEXURE C**

**AUTHORISATION OF INFORMATION OFFICER**

(In terms of the Promotion of Access to Information Act, 2000)

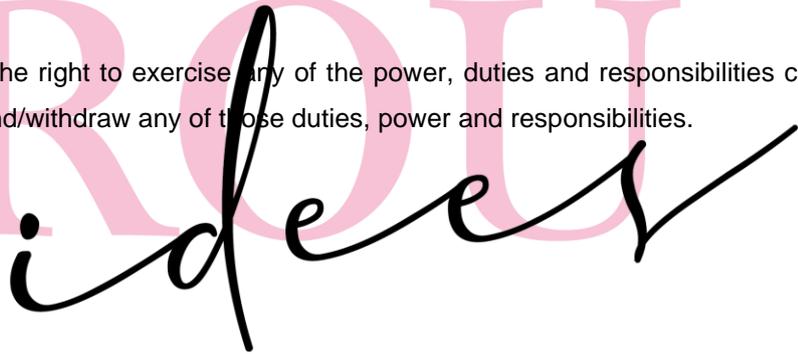
I, the undersigned

\_\_\_\_\_  
Information Officer

Hereby authorise \_\_\_\_\_ as an Information Officer of \_\_\_\_\_ and authorise you to exercise any of the powers, duties and responsibilities imposed on me by the Protection of Personal Information Act, 2013 and the Promotion of Access to Information Act, 2000.

Please be advised that I reserve the right to exercise any of the power, duties and responsibilities conferred herein, as well as the right to amend/withdraw any of those duties, power and responsibilities.

\_\_\_\_\_  
INFORMATION OFFICER



By my signature I hereby accept the authorisation of Information Officer.

\_\_\_\_\_  
AUTHORISED PERSON

DATE: \_\_\_\_\_