



**Protection of Personal Information (POPI) Act Company Manual**  
**(Including PAIA)**

---

Rev. 1.2, 23 September 2021

**POLICY STATEMENT**

- ✓ This policy forms part of **Kaimara (Pty) Ltd**, with company registration number **2018/419858/07** (policy owner) internal Company processes and procedures.
- ✓ Any reference to the “the Company” shall be interpreted to include the “policy owner” as well as all subsidiary divisions.
- ✓ The Company’s governing body, its employees, contractors, suppliers and any other persons acting on behalf of the Company are required to familiarise themselves with the policy’s requirements and undertake to comply with the stated processes and procedures.
- ✓ Risk owners and control owners are responsible for overseeing and maintaining control procedures and activities.

A handwritten signature in black ink, appearing to be 'P. Uys', written over a horizontal line.

**Pieter Uys**

6 October 2021

---

**Date**


# PROTECTION OF PERSONAL INFORMATION ACT (POPIA) OF 2013 MANUAL

## KAIMARA (PTY) Ltd

*(Hereafter referred to as the Company)*

Company Name:	Kaimara (Pty) Ltd
Company Registration Number:	2018/419858/07
VAT Registration Number (if applicable):	454 025 3848
Physical Address:	309 Brooks Street, Menlo Park, 0181
Postal Address:	309 Brooks Street, Menlo Park, 0181
Company Telephone Number:	+27 82 448 9662
Name of Information Officer:	Pieter Uys
e-mail Address of Information Officer:	<a href="mailto:pieter@kaimara.co.za">pieter@kaimara.co.za</a>

## Internal Document Approval

Information Officer Name	Signature	Date
Pieter Uys		28 September 2021

# Document Version Control

Version	Date	Summary of Changes
Rev 1.2	23 September 2021	Complete Company Manual Review as per legislation

## **Applicable National Legislation**

The Company recognizes that the Protection of Personal Information Act (POPIA) of 2013 does not exist in isolation and that POPIA acknowledges various rights regarding the processing of personal information in National legislation.

The daily operations of this Company areas of compliance *inter alia*: Business legislation (including all regulations issued in terms of such legislation):

- Basic Conditions of Employment Act No 75 of 1997 , Labour Relations Act No 66 of 1995, Occupational Health and Safety Act No. 85 of 1993 and other legislation commonly referred to as “Labour Law”
- Constitution of the Republic of South Africa 1996
- Companies Act No 71 of 2008
- Consumer Protection Act 68 of 2008
- Electronic Communications and Transactions Act 25 of 2002 (ECTA)
- The Cybercrimes Act 19 of 2020
- Promotion of Access of Information Act No 2 of 2000
- Income Tax Act 58 of 1962
- Value Added Tax Act No 89 of 1991
- South African Revenue Services Act 34 of 1997

**Table of Contents****Page**

Business Commitment and Process Info	6
Introduction	6
1. About us	7
2. Purpose of this policy Bundle	7
3. Principles	9
4. Adherence to this policy	9
5. Management Declaration	10
6. Definitions	11
7. Key Company Principles	15
8. Procurement of PI	17
9. Processing of PI	20
10. Further Processing	21
11. Retention and Restriction of Records	22
12. Security Safeguards	24
13. Security Compromises	25
14. Rights of Data Subjects	26
15. Request for Disclosure	28
16. Monitoring and Enforcement	28
17. Point of Contact	29
18. Standard Operating Procedures	29
19. Information Privacy Policy and Framework (POPIA and GDPR)	30
20. Information Transfer Policy	47
21. Duties and Responsibilities of Information Officer	53
22. Information Officer Appointment	55
23. Privacy Policy Statement	56
24. Client Privacy Notice	57
25. Annexure A Consent to gather PI	60
26. Annexure B Verification and Updating of PI	61
27. Annexure C Application for consent – Direct Marketing	62
28. Annexure D Consent for Direct Marketing	63
29. Annexure E Data subject consent withdrawal	64
30. Data Operators	65
31. Annexure F Notification to Third-party Data Operators	68
32. Annexure G Data Operator Privacy Policy Notice	69
33. Annexure H Data Operator Information Processing Agreement	73
<b>Policies</b>	
PE Prohibition on Processing of Special Personal Information	79
PF Prohibition on Processing of Special Personal Information regarding a data subject's Religious or Philosophical beliefs	80
PG Prohibition on Processing of Special Personal Information regarding a data subject's Race or Ethnic origin	81

PH	Prohibition on Processing of Special Personal Information regarding a data subject's Trade Union Membership	82
PI	Prohibition on Processing of Special Personal Information regarding a data subject's Political Persuasion	83
PJ	Prohibition on Processing of Special Personal Information regarding a data subject's Health or Sex Life	84
PK	Prohibition on Processing of Special Personal Information regarding a data subject's Criminal or Biometric Information	86
PL	Prohibition on Processing of Personal Information of Children	87
PM	Processing subject to Prior Authorisation	88
PN	Direct Marketing by means of Unsolicited Electronic Communication	89
PO	Transborder Information Flows	91

### **Additional Policies**

APA	Acceptable Use Policy	92
APB	Email Policy	97
APC	Handheld & Mobile Device Policy	100
APD	Access Control Policy	105
APE	Physical Security Policy	109
APF	Anti –Virus Policy	111
APG	Surveillance and Monitor Policy	112
APH	Data Retention Policy	115
API	Data Destruction Policy	119
APJ	Risk Management Policy	121
APK	Information Classification Policy	124
APL	Clean Desk and Clear Screen Policy	126
APM	Backup and Restoration Policy and Procedure	130
APN	Bring Your Own Device (BYOD) Policy	137
APO	Physical and Environmental Security Policy	142
APP	Disaster Recovery Policy	147

CONCLUSION	149
PAIA POLICY	150

## BUSINESS COMMITMENT AND PROCESS



## 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.

To manage and protect personal information the appropriate data security measures as well as procedures must be put in place and maintained.

This concept is not new but was there long before POPIA to prevent loss, theft or damage to personal information.

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 Company is committed to effectively managing personal information in accordance with POPIA's provisions.

## 1. About the company

Kaimara is a video production and photography studio. We focus on corporate video productions and photography, and also do wedding videos and photography.

Our work ethic and undertaking to all clients is to ensure that all instructions are dealt with timeously and with the proper care and skill in order to mitigate unnecessary costs and time wasting.

We are decidedly sensitive towards client confidentiality and are bound by all Ethical Rules and guidance's issued, most notably the duty to preserve client confidentiality, unless legislation or a court order provides otherwise.

## 2 Purpose of this Policy

The Protection of Personal Information Act 4 of 2013 ("POPI") gives effect to the constitutional right to privacy, regulates the manner in which personal information may be processed and provides rights and remedies to protect personal information.

- 2.1 As an employer as well as service provider and advertiser, the collection and processing of personal information is directly aligned to the execution of the Company purpose.
- 2.2 This Policy provides for what must and must not be done at the Company as regards personal information to which the Company becomes privy. The Policy in addition provides procedural guidelines, where appropriate, outlining how the Policy is to be implemented.

2.3 This POPI Policy must be adhered to by all key individuals including directors', employees and service providers. This purpose of this policy is to protect the Company from the compliance risks associated with the protection of personal information which includes:

- Breaches of confidentiality. For instance, the Company could suffer loss in revenue where it is found that the personal information of data subjects has been shared or disclosed inappropriately.
- Failing to offer choice. For instance, all data subjects should be free to choose how and for what purpose the Company uses information relating to them.
- Reputational damage. For instance, the Company could suffer a decline in shareholder value following an adverse event such as a computer hacker deleting the personal information held by the Company.
- This policy demonstrates the Company's commitment to protecting the privacy rights of data subjects in the following manner:
- Through stating desired behaviour and directing compliance with the provisions of POPIA and best Company.
- By cultivating a culture that recognises privacy as a valuable human right.
- By developing and implementing internal controls for the purpose of managing the compliance risk associated with the protection of personal information.
- By creating Company's that will provide reasonable assurance that the rights of data subjects are protected and balanced with the legitimate Company needs of the Company.



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

### 3 Principles

- 3.1 The primary purpose of the POPI Act is to regulate the collection and processing of personal information in a manner that will safeguard such information against unauthorised access and usage.
- 3.2 The purpose of this POPI Policy is to establish the requirements and conditions for the collection, distribution, and retention of personal information, in line with the prescripts of the POPI Act and the Promotion of Access to Information Act 2 of 2000 ("PAIA").
- 3.3 This Policy articulates the parameters in the collection, processing, storage, distribution and destruction of personal information by the Company, as aligned to the POPI Act. In addition, this Policy sets out how the Company deals with data subjects' personal information as well as the purposes for which personal information will be used. This Policy is made available by request from our Information Officer, whose details are provided below.

Pieter Uys - [pieter@kaimara.co.za](mailto:pieter@kaimara.co.za)

- 4 **The Company and its employees shall adhere to this policy** in the handling of all personal information received from, but not limited to natural persons, employees, clients, suppliers, agents, representatives and Company partners to ensure compliance with this Act, applicable regulations and other rules relating to the protection of personal information. The Act provides 8 conditions under which Personal Information may legally be gathered and processed.

Further, a POPIA policy and procedures manual will be required. It is the duty of the Responsible Person to ensure that these policies and procedures are followed.

One of the key aspects of any privacy law, and POPIA in particular, is that it describes the conditions for lawful processing. In other words, the conditions that need to be met if the company are to manage personal information correctly. **Meetings these conditions are mandatory and the company take cognisance hereof in an attempt to seek compliance to POPIA.**

## EIGHT CONDITIONS FOR LAWFUL PROCESSING



### 5. Management Declaration

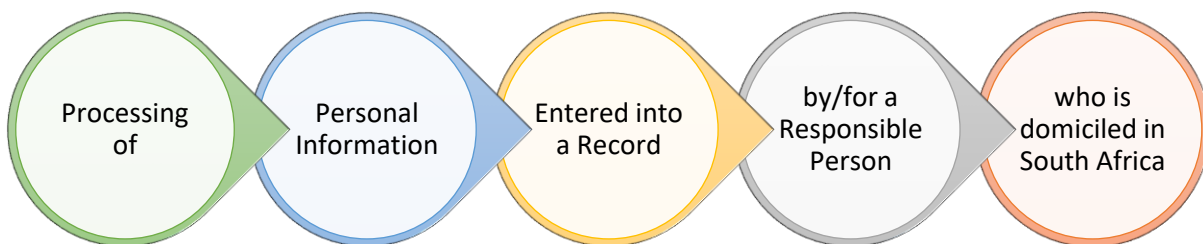
The Company, represented by the Information Officer confirms that we have familiarized ourselves with the content of this Act, applicable regulations and other rules relating to the protection of personal information, and will strive to adhere to these requirements at all times.

#### 5.1 This policy and its guiding principles applies to:

- The Company's governing body
- All branches, Company units and divisions of the Company
- All employees
- All contractors, suppliers and other persons acting on behalf of the Company

The policy's guiding principles find application in all situations and must be read in conjunction with POPIA as well 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:



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

- is concluded in the course of purely personal or household activities, or
- where the personal information has been de-identified.

## 6. Important Definitions

Term	Definition
Backup	Means the copying of physical or virtual files or databases to a secondary location for preservation to assist in the event of equipment failure or catastrophe.
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 ( <i>Section 1 of the Protection of Personal Information Act 4 of 2013</i> ).
Bring your own Device (BYOD)	Bring your own Device is the Company of allowing employees and other authorised persons that perform work for the Company to use their own personal devices for work purposes. This includes mobile phones, laptops, and tablets.
Company day	Shall mean any day other than a Saturday, Sunday, or Public Holiday in terms of the laws of the Republic of South Africa.
Child	Means a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him- or herself ( <i>Section 1 of the Protection of Personal Information Act 4 of 2013</i> ).
Company	Shall mean Kaimara Pty Ltd as specified on the Title page of this document.
Confidential Information	Confidential Information is a broader category than Personal Information ( <i>Please refer to the definition of Personal Information</i> ). This means that, as a rule, all Personal Information is confidential and should be kept confidential, but not all Confidential Information is necessarily Personal Information. Confidential means to be entrusted with another person's confidence or secret affairs.

Consent	Consent means any voluntary, specific, and informed expression of will in terms of which permission is given for the processing of Personal Information. <i>(Section 1 of the Protection of Personal Information Act 4 of 2013)</i>
Consumer	Shall mean any individual, client, customer, company, or any other legal entity making use of the services of the Company
Controls	Means control measures put in place by the Company to mitigate the risks identified to the security of Personal Information and / or Confidential Information, including instituting and implementing policies and procedures, management control, reporting, physical security measures and the like.
Data	Information that is entrusted with another person's confidence or secret affairs.
Data breach	A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or special category data transmitted, stored, or otherwise processed <i>(Section 1 of the Protection of Personal Information Act 4 of 2013)</i> .
Data Subject/s	Data subject means the person or Company to whom personal information relates <i>(Section 1 of the Protection of Personal Information Act 4 of 2013)</i> .
Data Subject Category	For Juristic and Natural Persons examples: customer/client category; supplier/service provider category; employee category; other (e.g., shareholders; members; stakeholders; non-executive directors).
Desk/s and Table	Means any physical working area where Personal Information and / or Confidential Information is processed, including printing areas, whether situated at the Company's premises or remotely.
Direct Marketing	Means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of promoting or offering to supply, in the ordinary course of Company, any goods or services to the data subject or requesting the data subject to make a donation of any kind for any reason <i>(Section 1 of the Protection of Personal Information Act 4 of 2013)</i> .
Electronic Communication	Means any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient <i>(Section 1 of the Protection of Personal Information Act 4 of 2013)</i> .
Filing System	POPI only applies to the processing of Personal Information which is in a record which forms part of a filing system. It is therefore important to know what a filing system is. A filing system is any structured set of Personal Information, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria <i>(Section 1 of the Protection of Personal Information Act 4 of 2013)</i> .
Information Incident	This means a single or a series of unwanted or unexpected events that threaten information security or privacy. Information Incidents include any collection, use, disclosure, access, disposal, or storage of information, whether accidental or deliberate, that is not authorised by the Company or the owner of such information <i>(Section 1 of the Protection of Personal Information Act 4 of 2013)</i> .
Information Matching Programme	Means the comparison, whether manually or by means of any electronic or other device, of any document that contains personal information about ten or more data subjects with one or more documents that contain personal information of ten or more data subjects, for the purpose of producing or verifying information that may be used for the purpose of taking any action in regard to an identifiable data subject <i>(Section 1 of the Protection of Personal Information Act 4 of 2013)</i> .
Information Officer	A Person appointed to implement the protection of the privacy of Personal Information in a Responsible Party or Company and the compliance of the POPI Act <i>(Section 1 of the Protection of Personal Information Act 4 of 2013)</i> .

Information Regulator / the Regulator	<p>There is hereby established a juristic person to be known as the Information Regulator, which:</p> <ul style="list-style-type: none"> <li>• Has jurisdiction throughout the Republic.</li> <li>• Is independent and is subject only to the Constitution and to the law and must be impartial and perform its functions and exercise its powers without fear, favour, or prejudice.</li> <li>• Must exercise its powers and perform its functions in accordance with this Act and the Promotion of Access to Information Act.</li> <li>• Is accountable to the National Assembly.</li> </ul> <p><i>(Section 39 of the Protection of Personal Information Act 4 of 2013)</i></p>
ISO27000 Series	Means the international standard for implementing an information security management system.
IT User	Means a User <i>(Please refer to the definition of User)</i> within the Company, authorised to be responsible for the carrying out of the Company's necessary Information Technology functions.
Juristic Person	Legal entity, e.g., company, close corporation, Company trust, homeowner's association, state-owned entity <i>(Section 1 of the Protection of Personal Information Act 4 of 2013)</i> .
Natural Person	Human being, e.g., sole proprietor, partners <i>(Section 1 of the Protection of Personal Information Act 4 of 2013)</i> .
Operator	An operator means a person who processes Personal Information for or on behalf of a Company in terms of a contract or mandate, without coming under the direct authority of that party <i>(Section 1 of the Protection of Personal Information Act 4 of 2013)</i>
Personal Data	Personal data is any Information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other identifiers.
Personal Data Breach	A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or special category data transmitted, stored, or otherwise processed.
Personal Information	<p>Personal information means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including:</p> <ul style="list-style-type: none"> <li>• Information relating to the race, gender, sex, pregnancy, marital status, national, ethnic, or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person.</li> <li>• Information relating to the education or the medical, financial, criminal or employment history of the person.</li> <li>• Any identifying number, symbol, email address, physical address, telephone number, location information, online identifier, or other assignment to the person.</li> <li>• The biometric information of the person.</li> <li>• The personal opinions, views, or preferences of the person.</li> <li>• Correspondence sent by the person.</li> <li>• The views or opinions of another individual about the person,</li> <li>• The name of the person if it appears with other personal information relating to the person.</li> </ul> <p><i>(Section 1 of the Protection of Personal Information Act 4 of 2013)</i></p>
Policy	A Statement that sets out the scope within one operates, it confirms what one can do, e.g., Privacy Policy.
Premises	The Company's premises or physical address, as per the Title Page of this document.
Procedure	A Statement that sets out how one implements a Policy, e.g., how the Company activities functions, and Company's could be the Privacy Impact Assessment Procedure.

Processing	<p>Processing means any operation or activity or any set of operations, whether by automatic means, concerning personal information, including</p> <ul style="list-style-type: none"> <li>• The collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation, or use.</li> <li>• Dissemination by means of transmission, distribution or making available in any other form.</li> <li>• Merging, linking, as well as restriction, degradation, erasure, or destruction of information.</li> </ul> <p>(Section 1 of the Protection of Personal Information Act 4 of 2013)</p>
Public Record	<p>A public record is a record that is accessible in the public domain, and which is in the possession of or under the control of a public body, whether it was created by that public body. (Section 1 of the Protection of Personal Information Act 4 of 2013)</p>
Record	<p>A record is any recorded Information regardless of form or medium:</p> <ul style="list-style-type: none"> <li>• Writing on any material.</li> <li>• Information produced, recorded, or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, and other device.</li> <li>• Any material subsequently derived from information so produced, recorded, or stored.</li> <li>• Label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means.</li> <li>• Book, map, plan, graph, or drawing.</li> <li>• Photograph, film, negative, tape or other device in which one or more visual images are embodied to be capable, with or without the aid of some other equipment, of being reproduced.</li> <li>• In the possession or under the control of a responsible party.</li> <li>• Whether or not it was created by a responsible party.</li> <li>• Regardless of when it came into existence.</li> </ul> <p>(Section 1 of the Protection of Personal Information Act 4 of 2013)</p>
Responsible Party	<p>A Responsible Party is a body or person who determines the purpose of and means for processing Personal Information. Included in this definition are juristic persons (e.g., companies and Companies), whether they are public or private organisations (Section 1 of the Protection of Personal Information Act 4 of 2013).</p> <p>For purposes for this manual “the Company” is deemed the “the Responsible Party”</p>
Restoration	<p>This means the process of restoring something to its former condition. In the case of a computer or other electronic device, means returning it to a previous state, including restoring a previous system backup or the original factory setting, or restoring data that was on the system.</p>
Screen/s	<p>This means any monitor on any device upon which Personal Information and / or Confidential Information is stored that displays such information.</p>
Security Incident	<p>Security Incident means any actual or potential accidental or unauthorised access, destruction, loss, alteration, disclosure, or any other unlawful forms of processing of Personal Information by the Company.</p>
Special Personal Information	<p>Special personal information means:</p> <ul style="list-style-type: none"> <li>• The religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject.</li> <li>• The criminal behaviour of a data subject</li> </ul> <p>(Section 26 of the Protection of Personal Information Act 4 of 2013)</p>

Security safeguards	<p>The responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent:</p> <ul style="list-style-type: none"> <li>• loss of, damage to or unauthorised destruction of personal information.</li> <li>• unlawful access to or processing of personal information.</li> </ul> <p>The responsible party must take reasonable measures to:</p> <ul style="list-style-type: none"> <li>• identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control.</li> <li>• establish and maintain appropriate safeguards against the risks identified.</li> <li>• regularly verify that the safeguards are effectively implemented.</li> <li>• ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.</li> </ul> <p>The responsible party must have due regard to generally accepted information security Company's and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations.</p> <p><i>(Section 19 of the Protection of Personal Information Act 4 of 2013)</i></p>
Unique Identifier	<p>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 (<i>Section 1 of the Protection of Personal Information Act 4 of 2013</i>).</p>
Users	<p>This is the employees, contractors, visitors, and / or other persons authorised to access and use the Company's systems</p>
Website	<p>A website is a collection of web pages and related content that is identified by a common domain name and published on at least one web server. Notable examples are Wikipedia.org, Google.com, and Amazon.com. All publicly accessible websites collectively constitute the World Wide Web.</p>

7. The Company's key principles in adhering to the requirements of the protection of personal information

The Company and its employees are committed to the following principles:

- To give effect to the constitutional right to privacy, by safeguarding personal information when processed by the Company, subject to justifiable limitations;
- To regulate the manner in which personal information may be processed, by establishing conditions, in harmony with international standards, that prescribe the minimum threshold requirements for the lawful processing of personal information;
- To be transparent in its standard operating procedures that govern the processing of personal information;

- To comply with the applicable legal and regulatory requirements regarding the processing of personal information;
- To collect personal information through lawful and fair means and to process personal information in a manner compatible with the purpose for which it was collected;
- Where required by law and according to local requirements, to inform data subjects when personal information is collected about them;
- Where required by law, regulations or guidelines, to obtain a data subject's consent prior to processing his/her/its personal information;
- To strive to keep personal information accurate, complete, up-to-date and reliable for its intended use;
- To strive to develop reasonable security safeguards against risks, losses, unauthorised access, destruction, use, modification or disclosure of personal information;
- To strive to provide data subjects with the opportunity to access the personal information relating to them and, where applicable, to comply with requests to correct, amend or rectify the personal information where incomplete, inaccurate or not compliant with the standard operating procedures;
- To only share personal information, such as permitting access, transmission or publication, with third parties (either within or outside the Company), only if reasonable assurance can be provided that the recipient of such information will apply suitable privacy and security protection to the personal information;
- To comply with any restrictions and requirements that applies to the Transborder Information Flow Policy.



## 8. Procurement of Personal Information

8.1 Personal information collected by the Company and/or any of its representatives, will be collected directly from the data subject, unless –

- a) The information is contained or derived from a public record or has deliberately been made public by the data subject;
- b) The data subject or a competent person where the data subject is a child, has consented to the collection of the information from another source;
- c) Collection of the information from another source would not prejudice a legitimate interest of the data subject;
- d) Collection of the information from another source is necessary –
  - I. To avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences;
  - II. To comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue;
  - III. For the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated;
  - IV. In the interest of national security; or
  - V. To maintain the legitimate interests of the Company or of a third party to whom the information is supplied;
- e) Compliance would prejudice a lawful purpose of the collection; or
- f) Compliance is not reasonably practicable in the circumstances of the particular case.

8.2 Personal information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the Company.

- 8.3 Steps will be taken to ensure that the data subject is aware of the purpose of the collection of the information.
- 8.4 The Company will take reasonably practicable steps to ensure that the personal information is complete, accurate, not misleading and updated where necessary, having regard to the purpose for which the personal information is collected and further processed.
- 8.5 Where personal information is collected from a data subject, the Company will take reasonably practicable steps to ensure that the data subject is aware of,
- a) The information being collected and where the information is not collected from the data subject, the source from which it is collected;
  - b) The name and address of the Company;
  - c) The purpose for which the information is being collected;
  - d) Whether or not the supply of the information by the data subject is voluntary or mandatory;
  - e) The consequences of failure to provide the information;
  - f) Any particular law authorising or requiring the collection of the information;
  - g) The fact that, where applicable, the Company intends to transfer the information to a third country or international organisation and the level of protection afforded to the information by that third country or international organisations;
  - h) Any further information such as the –
    - I. Recipient or category of recipients of the information;
    - II. Nature or category of the information;
    - III. Existence of the right of access to and the right to rectify the information collected;

IV. Existence of the right to object to the processing of personal information;

Which is necessary, having regard to the specific circumstances in which the information is or is not to be processed, to enable processing in respect of the data subject to be reasonable.

8.6 The steps referred to in clause 8.5 must be taken –

- a) If the personal information is collected directly from the data subject, prior to the information being collected, unless the data subject is already aware of the information as referred to in clause 8.5;
- b) In any other case, before the information is collected or as soon as reasonably practicable after it has been collected.

8.7 It will not be necessary for the Company to comply with clause 8.5 if –

- a) The data subject or a competent person if the data subject is a child has provided consent for the non-compliance;
- b) Non-compliance would not prejudice the legitimate interests of the data subject;
- c) Non-compliance is necessary –
  - I. To avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences;
  - II. To comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue;
  - III. For the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated; or
  - IV. In the interest of national security.
- d) Compliance would prejudice a lawful purpose of the collection;

- e) Compliance is not reasonably practicable in the circumstances of the particular case; or
- f) The information will –
  - I. Not be used in a form in which the data subject may be identified; or
  - II. Be used for historical, statistical or research purposes.

## 9. Processing of Personal Information

9.1 Personal information will only be processed lawfully and in a reasonable manner that does not infringe the privacy of the data subject.

9.2 Personal information may only be processed if –

- a) given the purpose for which it was processed, it is adequate, relevant and not excessive;
- b) the data subject or a competent person where the data subject is a child consents to the processing;
- c) processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party;
- d) processing complies with an obligation imposed by law on the Company;
- e) processing protects a legitimate interest of the data subject;
- f) processing is necessary for the proper performance of a public law duty by a public body; or
- g) processing is necessary for pursuing the legitimate interest of the Company or of a third party to whom the information is supplied.

9.3 In the event that the Company appoints or authorises an operator to process any personal information on its behalf or for any reason, it will implement necessary agreements to ensure that the operator or anyone processing personal information on behalf of the Company or an operator, must –

- a) Process such information only with the knowledge or authorisation of the Company; and
- b) Treat personal information which comes to his/her/its knowledge as confidential and must not disclose it, unless required by law or in the course of the proper performance of his/her/its duties.

9.4 The Company must maintain the documentation of all processing operations under its responsibility.

## 10. Further Processing of Personal Information

10.1 The Company must ensure that the further processing of personal information be compatible with the purpose for which it was collected.

10.2 To assess whether further processing is compatible with the purpose of collection, the Company will take account of –

- a) The relationship between the purpose of the intended further processing and the purpose for which the information was collected;
- b) The nature of the information concerned;
- c) The consequences of the intended further processing for the data subject;
- d) The manner in which the information has been collected; and
- e) Any contractual rights and obligations between the parties.

10.3 The further processing of personal information will not be incompatible with the purpose of collection if –

- a) The data subject or competent person where the data subject is a child, has consented to the further processing of the information;
- b) The information is available in or derived from a public record or has deliberately been made public by the data subject;
- c) Further processing is necessary –

- I. To avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences;
  - II. To comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue;
  - III. For the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated; or
  - IV. In the interest of national security;
- d) The further processing of the information is necessary to prevent or mitigate a serious and imminent threat to –
- I. Public health or public safety; or
  - II. The life or health of a data subject or other individual(s);
- e) The information is used for historical, statistical or research purposes and the Company ensures that the further processing is carried out solely for such purposes and will not be published in an identifiable form.

### **Types of Personal Information**

physical address	gender	pregnancy	education	correspondence	age	date of birth
opinions	health status	e-mail	marital status	language	identity number	employment history
disability	preferences	phone number	biometrics	name	others' opinions of you	

### **Types of Special Personal Information**

health information	sex life	religious beliefs	race	political persuasion
ethnic origin	criminal behaviour	philosophical beliefs	trade union membership	

## **11. Retention and Restriction of Records**

- 11.1 Records of personal information must not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed, unless –

- a) The retention of a record is required or authorised by law;
  - b) The Company reasonably requires a record for lawful purposes related to its functions or activities;
  - c) Retention of a record is required by a contract between the parties thereto; or
  - d) The data subject or a competent person where the data subject is a child has consented to the retention of a record.
- 11.2 Information collected or processed initially for the purposes of historical, statistical or research value, may be retained for a period longer than contemplated in clause 10.1, providing the Company has appropriate measures in place to safeguard these records against uses other than what it was intended for initially.
- 11.3 The Company will destroy or delete a record of personal information or de-identify it as soon as reasonably practicably after the Company is no longer authorised to retain a record.
- 11.4 The de-identifying or deletion of a record of personal information must be done in a manner that prevents its reconstruction in an intelligible/understandable form.
- 11.5 In the event that the Company uses a record of personal information of a data subject to make a decision about the data subject, it must –
- a) Retain the record for such period as may be required or prescribed by law or a code of conduct; or
  - b) If there is no law or code of conduct prescribing a retention period, retain the record for a period which will afford the data subject a reasonable opportunity, taking all considerations relating to the use of the personal information into account, to request access to the record.

- 11.6 The Company will restrict the processing of personal information if –
- a) Its accuracy is contested by the data subject, for a period enabling the Company to verify the accuracy of the information;
  - b) The Company no longer needs the personal information for achieving the purpose for which it was collected or subsequently processed, but it has to be maintained for purposes of proof;
  - c) The processing is unlawful and the data subject opposes its destruction or deletion and requests the restriction of its use instead; or
  - d) The data subject requests to transmit the personal data into another automated processing system.
- 11.7 Personal information that has been restricted may only be processed for purposes of proof, or with the data subject's consent, or with the consent of a competent person where the data subject is a child, or for the protection of the rights of another natural or legal person or if such processing is in the public interest.
- 11.8 Where personal information is restricted, the Company will inform the data subject before lifting the restriction.

## 12. Security Safeguards

- 12.1 The Company will secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable, technical and organisational measures to prevent –
- a) Loss of, damage to or unauthorised destruction of personal information; and
  - b) Unlawful access to or processing of personal information.
- 12.2 The Company will take responsible measures to –
- a) Identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;



- b) Establish and maintain appropriate safeguards against the risks identified;
  - c) Regularly verify that the safeguards are effectively implemented; and
  - d) Ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.
- 12.3 The Company will have due regard to generally accepted information security Company's and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations.
- 12.4 The Company will, in terms of a written contract between the Company and the operator, ensure that the operator which processes personal information for the Company, establishes and maintain the security measures as referred to in clause 12.1 – 12.3.
- 12.5 The operator will inform the Company immediately where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person.
13. Security Compromises
- 13.1 Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, the Company will notify –
- a) The Information Regulator; and
  - b) The data subject, unless the identity of such data subject cannot be established.
- 13.2 The notification of a breach will be made as soon as reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the Company's information system.

- 13.3 The Company will only delay notification of the data subject if a public body responsible for the prevention, detection or investigation of offences or the Regulator determines that notification will impede a criminal investigation by the public body concerned.
- 13.4 The notification to a data subject will be in writing and communicated to the data subject in at least one of the following ways:
- a) Posted to the data subject's last known physical or postal address; or
  - b) Sent by e-mail to the data subject's last known e-mail address; or
  - c) Placed in a prominent position on the website of the Company; or
  - d) Published in the news media.
- 13.5 The notification will provide sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise, including–
- a) A description of the possible consequences of the security compromise;
  - b) A description of the measures that the Company intends to take or has taken to address the security compromise;
  - c) A recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise; and
  - d) If known to the Company, the identity of the unauthorised person who may have accessed or acquired the personal information.

#### 14. Rights of the Data Subject

- 14.1 The data subject or competent person where the data subject is a child, may withdraw his, her or its consent to procure and process his, her or its personal information, at any time, providing that the lawfulness of the processing of the personal information before such withdrawal or the processing of personal information in terms of clause 9.2 (c) – (g), is not affected.

14.2 A data subject may object, at any time, to the processing of personal information—

- a) In terms of clause 9.2 (c) – (g), in writing, on reasonable grounds relating to his, her or its particular situation, unless legislation provides for such processing; or
- b) For purposes of direct marketing other than direct marketing by means of unsolicited electronic communications.

14.3 A data subject, having provided adequate proof of identity, has the right to –

- a) Request the Company to confirm, free of charge, whether or not the Company holds personal information about the data subject; and
- b) Request from the Company a record or a description of the personal information about the data subject held by the Company, including information about the identity of all third parties, or categories of third parties, who have, or have had, access to the information –
  - I. Within a reasonable time;
  - II. At a prescribed fee as determined by the Information Officer;
  - III. In a reasonable manner and format; and
  - IV. In a form that is generally understandable.

14.4 A data subject may, in the prescribed manner, request the Company to –

- a) Correct or delete personal information about the data subject in its possession or under its control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully; or
- b) Destroy or delete a record of personal information about the data subject that the Company is no longer authorised to retain.

14.5 Upon receipt of a request referred to in clause 14.4, the Company will, as soon as reasonably practicable –

- a) Correct the information;

- b) Destroy or delete the information;
- c) Provide the data subject, to his, her or its satisfaction, with credible evidence in support of the information; or
- d) Where an agreement cannot be reached between the Company and the data subject, and if the data subject so requests, take such steps as are reasonable in the circumstances, to attach to the information in such a manner that it will always be read with the information, an indication that a correction of the information has been requested but has not been made.

14.6 The Company will inform the data subject, who made a request as set out in clause 14.5, of the action taken as a result of the request.

15. Request for Disclosure

The Company will respond promptly when the data subjects request notification of purpose of use, disclosure, correction, addition or deletion of details, and suspension of use or elimination relating to personal information held by the Company.

16. Monitoring and Enforcement

Each employee of the Company will be responsible for administering and overseeing the implementation of this policy and, as applicable, supporting guidelines, standard operating procedure, notices, consents and appropriate related documents and processes.

Managers and responsible employees will be trained according to their functions in legal requirements, policies and guidelines that govern the protection of personal information in the Company. The Company will conduct periodic reviews and audits, where appropriate, to demonstrate compliance with privacy law and its policies, this Act and any applicable regulations.

Employees who violate the guidelines and standard operating procedures of this policy may be subject to disciplinary action being taken against him/her.

17. Point of Contact

The point of contact for requests, disclosures, questions, complaints and any other inquiries relating to the handling, collection, processing or re-identifying of personal information shall be directed to the Information Officer or Deputy Information Officer(s) as referred to in the Information Officer Policy.

18. Standard Operating Procedures

Each department will establish appropriate privacy standard operating procedures that are consistent with this policy, local customs and Companies as well as legal and regulatory requirements.

  
\_\_\_\_\_

**Pieter Uys**

6 October 2021

  
\_\_\_\_\_

**Date**

## **Information Privacy Policy and Framework**

### **(POPIA and GDPR)**

#### **1. STATEMENT**

- 1.1. Every person has rights with regard to how their personal information is handled and protected. In order to carry out its Company and provide its services, the Company may collect, store and process personal information about:
  - employees
  - clients;
  - consumers;
  - service providers / suppliers; and
  - Company contacts.
- 1.2. The Company recognises the need to treat this information in an appropriate and lawful manner. The Company is committed to complying with its obligations in this regard in respect of all personal information it handles, in a manner which maintains the confidence of the Company's clients, service providers / suppliers, Company contacts and employees.
- 1.3. The Protection of Personal Information Act no. 4 of 2013 ("POPIA") and regulations (2018) relate to identifiable, living, natural persons and identifiable, existing, juristic persons. The European Union General Data Protection Regulation ("GDPR") only relates to the information of European Citizens (natural persons). Additional privacy legislation may also be applicable should the Company also conduct Company in another country.
- 1.4. The types of information that the Company may be required to handle include details of current, past and prospective employees, service providers / suppliers, clients, consumers and other Company contacts that the Company communicates with. The information would typically include names, addresses, email addresses, dates of birth, identity / passport numbers, phone numbers, private and confidential information and, potentially, special personal information.

In addition, the Company may occasionally be required to collect and use certain additional types of personal information to comply with the requirements of the law.

- 1.5. The information may be stored on paper, electronically or by other media and is subject to certain legal safeguards specified in POPIA and GDPR, and potentially other applicable acts and regulations. The provisions of POPIA and GDPR impose restrictions on how the Company may collect and process the personal information in question.
- 1.6. This information privacy policy ("Policy") may be amended from time to time. Any breach of this Policy will be taken seriously by the Company and may result in disciplinary action being taken, which could include dismissal.

## **2. DEFINITIONS OF TERMS USED IN THIS POLICY**

### **2.1. POPIA Definitions**

- 2.1.1. "data subject" means all living, identifiable natural or juristic persons about whom the Company holds personal information or special personal information;
- 2.1.2. "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.
- 2.1.3. "personal information" means information relating to an identifiable, living, natural or juristic person, including (i) factual information, such as identity and passport numbers, names, addresses, phone numbers, email addresses and the like, or (ii) opinions regarding a data subject, such as a performance appraisal;
- 2.1.4. "processing POPIA" means any operation or activity, whether or not by automatic means, concerning personal information, including the:
  - collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use of personal information;
  - dissemination of such information by means of transmission, distribution or making available in any other form; or

- merging, linking, as well as restriction, degradation, erasure or destruction of information;

2.1.5. “responsible party” means a public or private body, or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information; and

2.1.6. “special personal information” means more sensitive information about an individual that pertains to racial or ethnic origins, political, religious or philosophical beliefs, health or sexual life, trade union membership or political persuasion, biometric information or criminal behaviour (to the extent that such criminal behaviour relates to the alleged commission by a data subject of an offence or any proceedings in respect of any offence allegedly committed by a data subject, which can only be processed under strict conditions and will usually require the express written consent of the data subject concerned.

## 2.2. GDPR Definitions

2.2.1. “controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

2.2.2. “personal data” means any information relating to an identified or identifiable natural person (“data subject”). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; and



- 2.2.3. “processing GDPR” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction; and
- 2.2.4. “processor” means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

### 3. **PURPOSE AND SCOPE OF THE POLICY**

- 3.1. This Policy sets out the Company’s general rules and the important legal conditions that must be satisfied in relation to the collecting, obtaining, handling, processing, storage, transportation and destruction of identifiable personal and special personal information.
- 3.2. This Policy also describes the privacy compliance framework and information governance of the Company in detail.
- 3.3. This Policy is applicable to all (i) employees, (ii) contractors, (iii) visitors, and / or (iv) other persons authorised to access and use the Company’s systems (“Users”).

### 4. **PRIVACY COMPLIANCE FRAMEWORK**

#### 4.1. **BACKGROUND**

- 4.1.1. To ensure compliance with the requirements of relevant privacy legislation such as POPIA and GDPR, the focus areas that must be addressed to be compliant are as follows:

- governance;
- people;
- process; and
- technology.

#### 4.2. **PRIVACY COMPLIANCE FRAMEWORK**

##### 4.2.1. Focus on governance

- The Company undertakes to take accountability for its actions by implementing good corporate governance.

- The focus on governance means that the Company will establish an Information Governance Committee (“IGC”) and other structures to ensure that data protection compliance is an ongoing process and that continued management of information processes takes place.

#### 4.2.2. Focus on process

- The Company undertakes to implement processes to ensure that personal information is processed in line with relevant legislation.
- This will include performing a Personal Information Impact Assessment (“PIIA”), as required by regulations promulgated under POPIA, and also developing and implementing the necessary policies and procedures and other control measures to ensure compliance with the relevant privacy legislation.

#### 4.2.3. Focus on people

- Most information security breaches involve people in one way or another. The Company undertakes to ensure that Users are made aware of their responsibilities in relation to processing personal information.
- Users must undergo privacy and information security training at least annually and all new employees must be appropriately trained within 3 (Three) months of commencing employment with the Company.

#### 4.2.4. Focus on technology

- The Company undertakes to implement technology with appropriate security safeguards. The reference to “technology” includes software, hardware and data specific requirements. Appropriate security technological safeguards must be in place where personal information is processed, stored and destroyed. The Company undertakes to appoint a specialist in information technology (“IT”) to set up and manage the Company’s technology. This will be done either by in-house employees or by outsourcing this IT function to a compliant third party.

#### 4.2.5. Review and audit

- Review and continuous monitoring: The Company will ensure that the following is reviewed and monitored on an ongoing basis:
  - That the Company's Governance Processes are functioning as intended and that regular IGC's have been established;
  - That the Company's processes have been reviewed on a regular basis and that all policies and procedures have been reviewed and updated at least annually;
  - That the Company's other control measures that have been implemented are functioning as intended and that they are adequate and effective;
  - That the Company's management and employees have been made aware and kept aware of how to process personal information and that a privacy awareness campaign has been developed and implemented;
  - That the Company's safety and security technology areas have undergone annual vulnerability assessments and, where applicable, that penetration testing has been done. This also includes information security management.
- Identify the gaps
  - On a regular basis, gaps or weaknesses ("Gap/s") should be identified and actions to mitigate such Gaps should be recorded in a Privacy Implementation Action Plan ("PIAP").
  - The Gaps should be prioritised and an accountable person should be appointed to rectify the Gaps.
  - A due date should be set by when the Gaps should be rectified.
- Action the gaps
  - The Gaps should be actioned in accordance with the PIAP.
  - A specific responsible person should be identified to co-ordinate or perform an action and a due date to complete the action in question should also be set.
  - Where there is a specific due date set, the progress to address the Gaps should be reported to the IGC.

- Audit the implementation
  - The Company undertakes to review the efficacy of the controls implemented to address and rectify the Gaps that have been identified.
  - The Company undertakes to ensure that the abovementioned review is conducted by an independent party not involved in the initial implementation. Where it is not possible to appoint an independent party within the Company then the review may be outsourced to independent third party auditors.
- Assess the outcome
  - The Company undertakes to assess the outcome of the audit and determine what action must be taken, if any, to address the Gaps. Where the Gap has been addressed and rectified, it must be noted. Where there is additional work required to be done, it must be added to the PIAP.
- Continuous reporting
  - The Company undertakes to continuously report the status of the management of personal information to the IGC and, at least on a quarterly basis, to the board of directors of the Company.

## 5. **INFORMATION GOVERNANCE**

### 5.1. **INFORMATION OFFICER**

5.1.1. The responsibilities of the information officer designated in terms of the POPIA include:

- the encouragement of compliance, such as awareness and training, by the Company, taking into consideration all of the conditions for the lawful processing of personal information;
- ensuring compliance by the Company with the provisions of POPIA;
- dealing with requests made to the Company in terms of POPIA, such as requests made from data subjects to update or view their personal information;
- working with the information regulator (“Regulator”) in relation to investigations; and

- the designation and delegation of relevant duties to deputy information officers appointed by the Company.

5.1.2. The responsibilities of the information officer have been expanded upon in the regulations promulgated under POPIA on 14 December 2018. In this regard, the information officer must ensure that:

- a compliance framework is developed, implemented, monitored and maintained;
- a PIIA is done to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information;
- a manual is developed, monitored, maintained and made available as prescribed in sections 14 and 51 of the Promotion of Access to Information Act 2 of 2000;
- internal measures are developed, together with adequate systems, to process requests for information or access thereto; and
- internal awareness sessions are conducted regarding (i) the provisions of POPIA, (ii) regulations promulgated in terms of POPIA, (iii) relevant industry codes of conduct, or (iv) information obtained from the Regulator.

## 6. **INFORMATION PROCESSING PRINCIPLES**

6.1. POPIA: The Company fully supports and complies with the 8 (Eight) protection principles of POPIA which are summarised below:

6.1.1. **Accountability:** a responsible party must ensure that the information processing principles are complied with;

6.1.1.1 The provisions of POPIA are intended not to prevent the processing of personal information, but to make sure that a responsible party ensures that the information processing principles as set out in POPIA, and all the measures that give effect to the principles, are complied with.

6.1.1.2. The data subject must be told the identity of the responsible party (in this case, the Company) and the purpose for which personal information is to be processed by the Company.

- 6.1.1.3. This Policy, developed by the Company to protect privacy, is available at the Company premises and is also accessible online at the Company's website. This Policy outlines the Company's commitment to privacy.
- 6.1.2. **Processing limitation**: personal information must be processed lawfully and in a reasonable manner;
- 6.1.2.1. For personal information to be processed lawfully, certain conditions have to be met. These may include, amongst other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the responsible party or the party to whom the personal information is disclosed. When special personal information is being processed, in most cases the data subject's explicit consent to the processing of such special personal information will be required.
- 6.1.2.2. A responsible party must collect personal information directly from the data subject unless (i) information is in a public record, (ii) the data subject has consented, (iii) the collection of personal information does not prejudice the legitimate interest of the data subject, or (iv) collection is necessary to comply with, or to avoid prejudice with or to the maintenance of, laws; to enforce legislation concerning the collection of revenue; for purposes of proceedings in a court; or in the interest of national security.
- 6.1.2.3. Where the Company processes personal information as a responsible party, the data subject should be informed of this fact. The data subject should also be informed for what purpose the personal information is being processed by the Company, and where or to whom such personal information may be disclosed or transferred.
- 6.1.3. **Purpose specification**: personal information must be obtained/processed for specific lawful purposes;
- 6.1.3.1. Personal information may only be processed for a specific and lawful purpose, or for any other purpose specifically permitted by POPIA, and steps must be taken to ensure that the data subject is aware of the purpose of the collection of the personal information.

The Company undertakes not to (i) collect personal information for one purpose and then use the personal information for another purpose, or (ii) retain personal information for any longer than is necessary for achieving the purpose for which the information was collected.

6.1.3.2. Personal information should only be collected to the extent that it is required for the specific purpose communicated to the data subject. Any personal information which is not necessary for that purpose should and will not be collected by the Company.

6.1.3.3. If it becomes necessary to change the purpose for which the personal information is processed, the data subject will be informed of the new purpose before any processing occurs.

Any employee personal information collected by the Company will be used for ordinary human resources purposes. Where there is a need to collect employee personal information for any other purpose, the Company will notify the employee in question of this and, where it is appropriate and practicable, the Company will get the employee's consent prior to such processing.

6.1.3.4. Where the Company collects personal information directly from a data subject, the personal information collected and processed by the Company, such as identity number, proof of address and the like, will only be used for the required purpose.

6.1.4. **Further processing limitation**: further processing of personal information must be in accordance or compatible with the purpose/s for which it was originally collected;

6.1.4.1. Personal information should not be kept longer than is necessary for the purpose for which it was collected. For guidance in relation to a particular personal information retention period, a User should contact the Company. The Company has various legal obligations to keep certain personal information of Users for a specified period of time. In addition, the Company may need to retain personal information for a period of time to protect its legitimate commercial and other interests.

6.1.4.2. The Company will not use any personal information for any purpose other than that for which it received the information in the first place, unless any further processing of such information is compatible with the original purposes for which the information was collected.

6.1.5. **Information quality**: personal information must be complete, accurate, not misleading and kept up to date;

6.1.5.1. Personal information must be complete, accurate, and kept up to date.

Personal information which is incorrect, or misleading is not accurate and steps will be taken to check the accuracy of any personal information at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date personal information will be destroyed. Employees should ensure that they notify their manager / human resources of any relevant changes to their personal information so that it can be updated and maintained accurately.

6.1.5.2. All personal information which is in paper form should be destroyed only by shredding.

If the personal information is held electronically, the Company must ensure that a reputable service provider destroys the personal information so that there is no future record of the information, and the Company must obtain an undertaking from the applicable service provider in this regard.

6.1.6. **Openness**: personal information may only be processed by a responsible party who has taken reasonable steps to notify the data subject;

6.1.6.1. Personal information may only be processed by the Company if the Company has notified the data subject that the Company has obtained the information from legitimate sources.

6.1.6.2. In cases where the Company works directly with a data subject, the Company will take reasonable, practicable steps to ensure that the data subject is aware of the following:

- What information is being collected and, where it is not collected from the data subject, the source of the information;
- The full name and addresses of the Company;
- The purpose for which the information is being collected;



- Whether supplying the personal information to the Company is voluntary or mandatory;
- The consequences of failure to provide the information;
- The applicable law authorising or requiring the collection of the information;
- The right to lodge a complaint against the Company the Regulator; and
- Any further relevant information, such as recipient or category of recipients of information, nature of information, existence of the right of access and the right to rectify information collection.

6.1.7. **Security safeguards**: personal information must be kept secure, and its confidentiality and integrity must be maintained;

6.1.8.1. The Company and its employees must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal information, and against the accidental loss of, or damage to, personal information.

6.1.8.2. The Company will put in place procedures and technologies to maintain the security of all personal information.

Personal Information may only be transferred to an operator if the operator has agreed to comply with those procedures and policies or has adequate security measures in place.

6.1.8.3. Users may refer to the Company's information security and related policies for further information concerning the Company's security safeguards.

6.1.8.4. The following principles must be maintained by the Company:

- Confidentiality: that only people who are authorised to use the personal information in question can access it. The Company will ensure that only authorised persons have access to an employee's personnel file and any other personal or special information held by the Company. Employees are required to maintain the confidentiality of any personal information and / or special personal information that they have access to.

- Integrity: that proper security safeguards are in place to ensure the maintenance and assurance, of the accuracy and consistency of information / data over its entire life cycle.
- Availability: that authorised users should be able to access the personal information if they need it for an authorised purpose.

6.1.8.5. Examples of security procedures at the Company include:

- Secure lockable desks and Cupboards – desks and cupboards must be kept locked if they hold confidential personal identifiable information of any kind;
- Methods of Disposal – paper documents must be shredded. CD-ROMs and USB keys should be physically destroyed when they are no longer required;
- Equipment – data users must ensure that individual computer monitors do not show confidential information to passers-by and that they log off from their computer when it is left unattended; and
- User Management – any access to the Company database is logged by the Company through a username and password system. Any changes / updates / uploads to the system are constantly tracked.

6.1.8.6. Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, the Company or any third party processing personal information under the authority of the Company, must notify the Regulator and the data subject as soon as is reasonably possible, taking into consideration the time that is taken by the Company to determine the scope of the breach and to restore the integrity of its information systems.

6.1.8.7. Any notification to a data subject must be in writing and communicated to the data subject in at least one of the following ways:

- Mailed to the data subjects last known physical or postal address;
- Sent by email to the data subjects last known email address;
- Placed in a prominent position on the website of the Company;
- Published in the news media; or

- As directed by the Regulator.

6.1.8.8. The notification referred to above must provide sufficient information to all the affected data subjects to take protective measures against the potential consequences of the security compromise including:

- a description of the possible consequences of the security compromise;
- a description of the measures that the Company intends to take or has taken to address the security compromise;
- a recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise; and
- if known to the Company, the identity of the unauthorised person who may have accessed or acquired the personal information in question.

6.1.8. **Data subject participation:** a data subject has the right to request the responsible party to confirm, free of charge, whether or not the responsible party holds personal information, together with a description of the personal information held by such responsible party.

6.1.9.1. A formal request from a data subject for information that the Company holds about them must be made in writing, accompanied with adequate proof of identification (in most instances, a certified copy of the individual's identity document or passport and proof of residence will be sufficient).

6.1.9.2. Any employees who receive a written request in respect of data held by the Company must forward it to the information officer immediately.

6.1.9.3. Any individual requesting personal information that may be held by the Company will be referred by the relevant employee to whom the request was made to the information officer, who will process the request. The information officer will either process the request directly, or will direct such employee to request a certified copy of the individual's identity document or passport as well as proof of address.

Once this is received, the employee will then be authorised to release the personal information to the individual. The employee must:

- record the request in the request register / system; and
- safely store the certified copy of the identity document and passport either in a file in a locked cupboard (if in paper format) or online in an encrypted folder which cannot be accessed by unauthorised personnel. Storage of these documents should be kept for 1 (one) year, after which they must be properly destroyed.

6.1.9.4. Any employee dealing with telephonic enquiries from data subjects should guard against disclosing any personal information held by the Company over the phone. In particular, the employee must:

- check the identity of the caller to ensure that information will only be given to a person who is entitled to that information – this can be accomplished by confirming: identity number, date of birth, address, cell phone number and the like;
- request that the caller put their request in writing if the employee is not completely sure about the identity of the caller and in circumstances where the identity of the caller cannot be verified. In these circumstances, the employee should also request that a certified copy of the identity document / passport of the individual is provided before information is released;
- refer the request to their manager for assistance in difficult situations. No employee should feel forced to disclose personal information; and
- where a request has been made in terms of this section, and personal information is communicated to the data subject, the data subject must be advised of their right to request the correction of the information.

6.1.9.5. The data subject may request that the Company correct or delete personal information which is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully, or to destroy such record of personal information.

If such a request is made, the Company must send this request to the appropriate party within the Company who should then correct the information, destroy or delete it, and provide the data subject with credible evidence that this has been done.

## 6.10. GDPR

6.10.1. The Company fully supports and complies with the 6 (Six) protection principles of the GDPR which are summarised below:


- Lawfulness, fairness and transparency: The personal information of the European citizens will be processed lawfully, fairly and in a transparent manner in relation to the data subject.
- Purpose limitation: The personal information of the European citizens will be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for achieving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purpose.
- Data Minimisation: The personal information of the European citizens will be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accuracy: The personal information of the European citizens will be accurate and, where necessary, kept up to date.
- Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purpose for which it is processed, is erased or rectified without delay.
- Storage Limitation: The personal information of the European citizens will be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.

Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1), subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject.

- Integrity and Confidentiality: The personal information of the European citizens will be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

7. **REVIEW OF POLICY**

The Company will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives on at least an annual basis and more frequently if required, taking into account changes in the law and organisational or security changes.

---

  
**Pieter Uys**

6 October 2021

---

**Date**

## **Information Transfer Policy**

### **1. INTRODUCTION**

- 1.1. This policy regulates the transfer of information within and from and to the Company.
- 1.2. Where the information being transferred comprises personal information as this term is defined in the Protection of Personal Information Act 4 of 2013 (“Personal Information”), the provisions of POPIA will apply to the processing of such Information by or on behalf of the Company.

### **2. PURPOSE**

- 2.1. There are many occasions when information is transferred between different departments of the Company, and between the Company and third-party service providers, clients, clients and the like. This transfer of information is affected by a wide variety of media and methods, in both electronic and paper format. In every transfer of information, there is a risk that the information in question may be lost, misappropriated or accidentally disclosed. Where the information in question is (i) Personal Information, and / or confidential, sensitive, critical or proprietary information of the Company (“Confidential Information”) the risk to the Company increases significantly.
- 2.2. The Company often has a duty of care in handling information. For this reason, and because of its legal obligations under POPIA, the Company considers it imperative to maintain the trust of its stakeholders and partners. It is, therefore, essential that the transfer of information is performed in a way that adequately protects such information.
- 2.3. It is at all times the responsibility of the sender of information to assess the risks involved in the transfer of such information and to ensure that adequate controls are in place to mitigate such risks.

Where the sender of information delegates the final actual task of sending information to untrained or inexperienced staff, the original sender remains responsible for ensuring that the transfer of information complies with this Policy.

This Policy outlines the responsibilities attached to, and the minimum-security requirements, for the transfer of information, including (i) Personal Information, and / or (ii) Confidential Information.

### 3 **SCOPE AND USERS**

- 3.1. This policy applies to all departments where (i) Personal Information, and / or (ii) Confidential Information is created, accessed, processed, updated, stored, maintained or managed.
- 3.2. This Policy applies to all (i) employees, (ii) contractors, (iii) visitors, and / or (iv) other persons authorised to access and use the Company's systems ("Users") who are in any way involved in the transfer of information as contemplated by this Policy.
- 3.3. Unless the contrary is specified, to the extent that any terms used in this Policy are defined in POPIA, such terms will be given the meaning ascribed to them in POPIA.

### 4. **REFERENCE DOCUMENT**

This policy should be read in conjunction with the Company's other policies that regulate the security of information, including, without limitation, the Acceptable Usage Policy.

### 5. **POLICY**

- 5.1. Electronic communication channels
  - 5.1.1. The Company's information may be exchanged through the electronic communication channels outlined below.
  - 5.1.2. New data channels must be approved by the information officer (IO) of the Company prior to being implemented. A data channel is either a physical transmission medium, such as a wire transfer, or a logical connection over a multiplexed medium, such as a radio channel ("Data Channel"). The IO's approval will set out the (i) type of communication allowed, and (ii) controls pertaining to the use of the Data Channel.



Public information may be made available to the public, but all information meant for internal use only may only be transferred to parties that are authorised by the Company to receive such information and that are bound contractually not to disclose such information, whether by employment agreements or appropriate non-disclosure agreements.

5.1.3. Where the information is classified as either (i) Personal Information, and / or (ii) Confidential Information, the relevant Data Channels and other guidelines set out below should be used to ensure that such information is transferred in a secure manner and that only certain secure channels are used to transfer such Information.

- Email may be used to transfer (i) Personal Information, and / or (ii) Confidential Information only when such information has been sufficiently password protected or properly encrypted in the email in question;
- A file transfer method may be used to transfer (i) Personal Information, and / or (ii) Confidential Information only when a secure file transfer protocol (known as a “SFTP”) channel is used;
- Portable Media (such as CDs, DVDs, USB drives and memory cards) may be used to transfer (i) Personal Information, and / or (ii) Confidential Information only when such information on the device in question is properly password protected or encrypted; and
- Telephonic communication, fax transmission, mobile voice or sms communication, and / or social media may not be used to transfer or disclose (i) Personal Information, and / or (ii) Confidential Information.

5.2. Non-electronic communication channels

5.2.1. The Company’s information may be exchanged through the non-electronic communication channels outlined below.

5.2.2. Public information may be made available to the public, but all information meant for internal use only may only be transferred to parties that are authorised by the Company to receive such information and that are bound contractually not to disclose such information, whether by employment agreements or appropriate non-disclosure agreements.

5.2.3. Where the information is classified as either (i) Personal Information, and / or (ii) Confidential Information, the guidelines set out below should be used to ensure that such information is transferred in a secure manner and that only certain secure channels are used to transfer such Information.

- Registered or normal post may not be used to transfer (i) Personal Information, and / or (ii) Confidential Information; and
- Letters delivered by hand may be used to transfer (i) Personal Information, and / or (ii) Confidential Information only when the sender of such information ensures that the party receiving the information is properly identified and authorised to receive such information.

## 6. **RESPONSIBILITIES OF THE SENDER AND RECEIVER OF INFORMATION**

6.1. The sender's responsibilities for transferring (i) Personal Information, and / or (ii) Confidential Information are:

- 6.1.1. assessing the information to be sent and ensuring that it is in line with the guidelines set out in this Policy;
- 6.1.2. ensuring that the identity of the receiver is known, that such receiver is authorised to receive the information and that the channel used for the transfer is conducive to transfer the information to that person;
- 6.1.3. ensuring that the transfer of information is formally confirmed and documented; and
- 6.1.4. ensuring that the information is sent and tracked in an appropriate manner to ensure compliance with this Policy.

6.2. The person receiving (i) Personal Information, and / or (ii) Confidential Information is responsible for ensuring that:

- 6.2.1. the information received is information that they have a right to receive; and
- 6.2.2. they fully disclose their identity.

## 7. **RELATIONSHIP WITH EXTERNAL PARTIES**

7.1. Before exchanging any information with any person or party outside of the Company, an agreement must be concluded between the Company and such third party. Such agreement must comply with POPIA and must contain at least the following clauses:

- 7.1.1. Method of identification of the third party;
- 7.1.2. Confirmations or warranties regarding authorisation to access information;
- 7.1.3. Technical standards and appropriate Data Channels for the transfer of information;
- 7.1.4. Labelling and handling of (i) Personal Information, and / or (ii) Confidential Information;
- 7.1.5. Warranties from the third-party regarding compliance with POPIA and all other relevant privacy laws;
- 7.1.6. Obligations on the third party to safeguard the security of the information in question;
- 7.1.7. Indemnities in favour of the Company in the event of a breach by the third party of POPIA or the agreement itself;
- 7.1.8. Protections for the Company's intellectual property rights; and
- 7.1.9. Incident responses and what must be done in the event of security breaches.

## 8. **RIGHTS RESERVED BY THE COMPANY**

The Company reserves the right to monitor, audit, screen, and preserve Company information as the Company deems necessary, in its sole discretion, in order to maintain compliance with this Policy and, by extension, all relevant provisions of POPIA. Any dissemination, unauthorised use or benefit from any Company information by a User in contravention of this Policy may result in disciplinary action being taken against such User by the Company. Furthermore, the use of any account or system in such a way that breaches any of the provisions of this Policy will be reported to the appropriate supervisor or manager within the Company, which may lead to further disciplinary action being taken.

## 9. **ENFORCEMENT AND POTENTIAL DISCIPLINARY ACTIONS**

Any violation of this Policy may result in disciplinary action being taken against the User in question. Such disciplinary action will be taken in accordance with the Company's applicable disciplinary code, and may include the (i) termination of employment in relation to employees of the Company, or (ii) cancellation or termination of contractual relations in the case of other Users, such as contractors or consultants.

Notwithstanding the foregoing, should any authorised User fail to adhere to this policy, the individual will be dealt with as prescribed by the Company's disciplinary code and procedures.

10. **POLICY AWARENESS AND UPDATE**

- 10.1. Training and awareness: The (i) requirement for, and (ii) a User's obligation in terms of, this Policy will be explained in detail in the Company's induction program, in the case of employees of the Company. Further training and additional awareness regarding the Policy will be offered from time to time by the Company. The Company will specifically make Users who are not employees of the Company aware of the Policy.
- 10.2. Dissemination: This Policy will be made available on the Company's network, intranet or similar portals.
- 10.3. Review: This Policy will be reviewed from time to time in order to ensure ongoing compliance with POPIA, but such revisions will take place at least annually. More frequent review may be required in response to (i) exceptional circumstances, (ii) organisational change, or (iii) relevant changes in legislation or guidance.



**Pieter Uys**

6 October 2021

**Date**

## **Duties and Responsibilities of Information Officer**

### 1. Appointment of Information Officer

The Information Officer in terms of the Company's structure will be the Company Director/Owner.

### 2. Registration as Information Officer


The Information Officer shall ensure that he/she is registered with the Regulator within the prescribed manner and timeframe, as being the Information Officer of the Company.

### 3. Duties and Responsibilities of the Information Officer

The Information Officer's responsibilities include:

- a) Ensuring compliance by the Company with the Company's policies regarding the protection of personal information and the provisions of this Act. Taking steps to ensure the Company's reasonable compliance with the provision of POPIA.
- b) Keeping the governing body updated about the Company's information protection 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 Company's personal information processing procedures. This will include reviewing the Company's information protection procedures and related policies.
- d) Ensuring that POPI Audits are scheduled and conducted on a regular basis.
- e) Ensuring that the Company makes it convenient for data subjects who want to update their personal information or submit POPI related complaints to the Company. For instance, maintaining a "contact us" facility on the Company'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 Company. This will include overseeing the amendment of the Company'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 Company are fully aware of the risks associated with the processing of personal information and that they remain informed about the Company'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 Company.
- j) Addressing employees' POPIA related questions.
- k) Addressing all POPIA related requests and complaints made by the Company'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.

---

Pieter Uys

6 October 2021

---

Date

## INFORMATION OFFICER APPOINTMENT LETTER

The company herewith and with immediate effect appoint you as the Information Officer as required by the Protection of Personal Information Act (Act 4 of 2013). This appointment may at any time be withdrawn or amended in writing.

You are entrusted with the following responsibilities:

- Taking steps to ensure the organisation's reasonable compliance with the provision of POPIA.
- Keeping the governing body updated about the organisation's information protection 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.
- Continually analysing privacy regulations and aligning them with the organisation's personal information processing procedures. This will include reviewing the organisation's information protection procedures and related policies.
- Ensuring that POPI Audits are scheduled and conducted on a regular basis.
- Insuring that the organisation makes it convenient for data subjects who want to update their personal information or submit POPI related complaints to the organisation, to do so. For instance, maintaining a "contact us" facility on the organisation's website.
- 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 organisation's employment contracts and other service level agreements.
- Encouraging compliance with the conditions required for the lawful processing of personal information.
- Ensuring that employees and other persons acting on behalf of the organisation are fully aware of the risks associated with the processing of personal information and that they remain informed about the organisation's security controls.
- Organising and overseeing the awareness training of employees and other individuals involved in the processing of personal information on behalf of the organisation.
- Addressing employees' POPIA related questions.
- Addressing all POPIA related requests and complaints made by the organisation's data subjects.
- 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.

**I hereby accept the appointment as Information Officer I understand the implications of the appointment and confirm my acceptance of this appointment. I have studied the relevant sections of the POPIA and associated Regulations and understand what is required of me.**

**Pieter Uys**

Name & Surname

Signature



6 October 2021

Date

## **POPIA Privacy Policy Statement**

In South Africa, consumers have a deep mistrust and lack the confidence that organisations use the information they collect lawfully and for an agreed upon purpose. The Protection of Personal Information Act (POPIA) of 2013 is South Africa's new data protection law. It joins a raft of similar laws around the world.

We, the Company, believe the consumer privacy is something that they never have to question. It should be simple, straightforward, and understood. Therefore, the Company builds its Privacy Policy Statement on these three objectives:

- Respect for consumer privacy.
- Provision of transparency on information processing.
- Provision of security as it relates to cybertheft, data loss and identity theft.

We believe that privacy should be focused on private consumer interactions, data encryption, reducing data permanence, data safety, interoperability of devices and applications, and secure data storage. We take full responsibility in terms of the Protection of Personal Information Act of 2013 (POPIA) to take reasonable measures to ensure data security and prevent data breach or loss.

POPIA is about security, in addition to being about respecting the rights of the data subject.

The Company shall promote a culture of data privacy and digital transformation as a vital strategy in the complexity of our daily operations. This would deliver a competitive advantage to the Company soon. The Company acknowledges that there is no single tool that can accomplish end-to-end POPIA compliance, but that it is only possible through the ethical conduct of employees and managers, and the security and maintenance of our data protection systems.

---

**Pieter Uys**  
**Information Officer**

6 October 2021

---

**Date**



## **PRIVACY NOTICE**

The Company recognises that one of its fundamental responsibilities is to ensure that it protects Personal Information entrusted to it by its clients. This is critical for the Company's reputation and for complying with its legal obligations.

This Notification complies with the Protection of Personal Information Act 4 of 2013.

### **1. Applicability**

The Company collects three types of Information:

#### **1- Personal Information.**

Personal Information means any information that relates to a person, that can identify such person, for example, telephone number, name, address, transaction history, etc.

#### **2- Sensitive Personal Information.**

Sensitive Personal Information of a person means such personal information which consists of information relating to passwords, financial Information such as bank account or credit card or debit card or other payment instrument details. Also, sexual orientation, physical physiological and mental health condition, medical records and history and biometric Information. It also includes national identifiers including account number, bank card details, passport number, income, etc.

#### **3- Non-personal Information.**

### **2. Accuracy**

The Company has processes in place to ensure that the Personal Information it stores is complete, accurate and current. If there is a reason to believe that Personal Information residing with the Company is incorrect, the customer should inform the Company in this regard. The Company shall correct the information as quickly as possible.

### 3. **Purpose of Collection of Personal Information**

The Company will use the information collected to manage its Company and offer an enhanced experience. It will also enable the Company to:

- Process applications, requests, and transactions.
- Maintain internal records.
- Provide services to clients, including responding to Client / customer requests.
- Comply with all applicable laws and regulations.
- Recognise the Client / customer when he/she make payments to the Company.
- Understand the needs of the Client / customer, and provide relevant product and service offers.

If a customer does not wish to provide consent for usage of its Personal Information or Sensitive Personal Information or later withdraws the consent, the Company shall have the right not to provide services or to withdraw the services for which such information was sought from the customer.

### 4. **Sharing of Information**

The Company shall not share the Personal Information of its clients without their prior consent. If the Company shares the Personal Information to third-parties, these parties shall be bound contractually to ensure that they protect customer Personal Information in accordance with applicable laws.

The above obligations shall not apply to information shared with government mandated under the law. If any Personal Information freely available or accessible in the public domain, the Company shall not have any obligations regarding its protection.

### 5. **Security**

The security of Personal Information is a priority and shall be ensured by maintaining physical, electronic, and procedural safeguards. These safeguards must meet applicable laws to protect customer information against loss, misuse, damage and unauthorised access, changes, or sharing.

Employees shall be trained in the proper handling of Personal Information.

When other companies are used to provide services on behalf of the Company, we shall ensure that such companies protect the confidentiality of Personal Information they receive in the same manner the Company protects it.

6. **Amendments**

The Company reserves the right to change or update this Notification, at any time with reasonable notice to clients on Company's website or by notice at the Company. Clients will always be aware of the information that is collected, for what purpose the Company uses it, and under what circumstances, the Company may disclose it.

7. **Response to Enquiries and Complaints**

The Company encourages Client / customer enquiries, feedback and complaints which shall help it identify and improve the services provided to the clients. Should you have any enquiries, please contact the Information Officer of the Company.

---

Pieter Uys

6 October 2021

---


Date

**ANNEXURE A: CONSENT TO GATHER PERSONAL DATA**

I Petrus Johannes Uys (Full Names) hereby consent to the collection, processing and sharing of my personal information as contemplated in the Protection of Personal Information Act No 4 of 2013 by the company, their staff and third parties with whom the company has a contractual relationship for the following purposes:

- i. rendering and managing services offered in terms of a client – service provider relationship;
- ii. the administration of the contractual relationship between myself and the company ;
- iii. communicating with other persons inasmuch as it relates to my services and the management thereof;
- iv. collecting monies owing from me.”

Signed at Pretoria on this 6th day of October 2021

Full Name:	Petrus Johannes Uys
Signature:	

## **ANNEXURE B: VERIFICATION AND UPDATING OF PERSONAL INFORMATION**

Dear Consumer,

Enclosed is your Personal Information that we have on record.

Kindly confirm that it is correct. If it is incorrect or requires updating, please amend it accordingly.

When completed, email to our Information Officer.

### **Changes in Personal Information**

If there are any further changes or updates, kindly use this form and email to our Information Officer.

If you require any further Information or clarification, kindly contact the Information Officer.

Thank you,

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

**ANNEXURE C: APPLICATION FOR CONSENT TO DO DIRECT MARKETING****CLIENT / PROSPECT / SUPPLIER DETAILS**

Full Name:	
Date of Birth:	
ID nr / Passport Nr:	
Contact Nr:	
Email:	
Relationship to the Company:	

**REQUEST FOR CONSENT TO RECEIVE DIRECT MARKETING MATERIAL IN TERMS OF SECTION 69(2) OR REGULATION 6 OF THE POPI ACT**

Dear Consumer,

We periodically send out newsletters and other relevant information using electronic means that could be of benefit to you. As this communication is classified as Direct Marketing in terms of the POPI Act, we would appreciate your consent that you would like to receive these communications and retain your details on our communication list.

If you would like to receive these communications, kindly sign off on the attached form and send it back to us.

We look forward to being of service to you.

With kind regards




---

Information Officer

**ANNEXURE D: CONSENT FROM DATA SUBJECT FOR DIRECT MARKETING**

I, \_\_\_\_\_ (Full names), hereby give my consent to receive direct marketing of goods or services to be marketed by means of electronic communication.

Specify method of communication with an x:

<input type="checkbox"/>	Fax
<input type="checkbox"/>	E-mail
<input type="checkbox"/>	SMS
<input type="checkbox"/>	Mail

Signed at \_\_\_\_\_ on this \_\_\_\_\_ day of \_\_\_\_\_ 20\_\_

Full Name:	
Signature:	

*Kindly send this Consent Form to the Information Officer of the Practice.*

**ANNEXURE E: DATA SUBJECT CONSENT WITHDRAWAL FORM**

I, (Full Name) \_\_\_\_\_,

would like to withdraw my consent to process my Personal Information by the company. Therefore, the company no longer has my consent to process my Personal Information for the purpose of

\_\_\_\_\_  
 \_\_\_\_\_  
 (specify legitimate reason of processing Personal Information), which was previously granted.)

The withdrawal of consent does not affect the lawfulness of the processing activities up to this point.

Please provide the following Information to help us identify you in our systems:

**My Personal Information, as Data Subject, is as follows:**

Full Name:	
Date of Birth:	
ID nr / Passport Nr:	
Contact Nr:	
Email:	
Relationship to the Company:	

Signed at \_\_\_\_\_ on this \_\_\_\_\_ day of \_\_\_\_\_ 20\_\_\_\_

Full Name:	
Signature:	

*Form to the Information Officer of the Company.*



## **Data Operators**

### **1. PURPOSE**

The control of risks introduced into the Company by contractors, service providers, accountants, consultants, third-parties and suppliers (Data Operators) is an important element of the Company risk management system.

For the purposes of this Policy Data Operator means any organisation whom the Company pays in return for any type of goods or service, or the processing of Personal Information. Selection criteria for Data Operators are dependent on the nature of the goods or services to be supplied and are determined by the Company policies and procedures plus statutory requirements.

This Policy defines the duties of the Data Operator in terms of the processing of Personal Information on behalf of the Company in compliance with the Protection of Personal Information Act, No.4 of 2013.

This Policy must be read in conjunction with the *Acceptable Usage Policy*. Confidentiality Agreements and Non-Disclosure Agreements referred to in the Acceptable Usage Policy, will be found in the Annexure of this Policy as it relates to Data Operator Personal Information as well as processing of Personal Information by Data Operators (*Refer to Annexure C and D*)

### **2. INTRODUCTION**

If the Company uses Data Operators to process Personal Information, it must comply with Sections 20 and 21 of the Protection of Personal Information Act. POPIA requires the Company to enter into a written agreement with a Data Operator that processes Personal Information for the Company. The Company must ensure that such Data Operator maintains the security measures required by POPIA.

### **3. GUIDANCE FOR REVIEWING & MONITORING DATA OPERATORS**

#### **POPIA and Data Security Policies**

The first stage in the process is to see if the Data Operator has the right attitudes to the security of Personal Information, and this is done by checking their policies.

**a) Competence**

Next a check should be carried out to ensure that the Data Operator are capable of processing Personal Information in a responsible manner and supplying services that meet appropriate legal requirements.

**b) Standards**

Once it is established that Data Operator can work in accordance with POPIA requirements, the Company needs to check that the product or service the Data Operator will supply is of a high enough standard.

**c) Monitoring**

Checks on policies, competence and standards must take place before the Data Operator's 'offer' (usually a quote, whether verbal or written) is accepted by the Company. There will be a need to monitor Data Operators' work to ensure that they are complying with the agreed methods and risk control measures. Also, that execution of the service is performed in accordance with proposed methods and control measures. Verification of the service takes place throughout service delivery. These checks complete the selection process. As soon as verification that the purchased product or services meet specified POPIA requirements is completed, the Data Operator can then be contracted under the Company's existing day-to-day POPIA controls.

**4. DATA OPERATOR DUTIES**

The Data Operator agrees to the following (further details of which can be found in the section headed *Information Processing Agreement (Refer to Annexure E)*):

- Only use and disclose the Personal Information in accordance with the Company's specific written instructions.
- Take reasonable and appropriate, organisational, and technical security measures to protect Personal Information supplied by the Company or otherwise made available to the Data Operator.
- Permit the Company to audit the Data Operator in terms of its compliance with Sections 19 to 21 of POPIA.

- Comply with requests by the Company for access to Personal Information following the receipt of a valid and approved Data Subject Request.

The Data Operator is not permitted to sub-contract any of the processing of the Personal Information supplied by the Company, without first:

- Ensuring the sub-contractor will be compliant with the requirements of Sections 19 to 21 of POPIA.
- Obtaining prior written permission of the Company .

The Data Operator must also agree to co-operate with any action required to fulfil the requests or demands of the Information Regulator as outlined in POPIA, whether directly by the Information Regulator or indirectly by the Company.

## 5. **RIGHTS OF THE COMPANY**

An audit of the compliance of the Data Operator with Sections 19 to 21 of POPIA to be conducted by the Company, may include but is not limited to:

- Ensuring that the Data Operator transfers data securely.
- Ensuring that the Data Operator reports any security breaches or other problems to the Company.

In any other way fulfil the duties of the Company as outlined in Section 21 of POPIA.

## 6. **TERMINATION OF INFORMATION PROCESSING AGREEMENT**

In terms of processing of Personal Information:

- Where the Data Operator is found by the Information Regulator to have not fulfilled its obligations in terms of compliance with POPIA, the Company has the right to cancel the Information Processing Agreement with the Data Operator with immediate effect.
- Whether for fault or any other termination reason, the Data Operator must return all Personal Information processed on behalf of the Company without delay, unless the Data Operator is required to retain such records in terms of other legislation or regulations.

**ANNEXURE F: NOTIFICATION TO THIRD-PARTY DATA OPERATORS****THIRD PARTY CLIENT /SUPPLIER / SERVICE PROVIDER/VENDOR CONTACT DETAILS:**

Data Operator Name:	
Data Operator Registration Number:	
VAT Registration Number (if applicable):	
Physical Address:	
Name of Information Officer:	
Email Address of Information Officer:	
Date:	

**DATA OPERATOR SERVICES AND THE PROTECTION OF PERSONAL  
INFORMATION ACT 4 OF 2013**

Your organisation as vendor, third-party client, supplier, or service provider, has been identified as a Data Operator in terms of the POPI Act.


A Data Operator is a Third-Party independent organisation that processes Personal Information on behalf of the Company.

The Company will send the Data Operator Personal Information Processing Agreement, which is a statutory requirement in terms of the POPI Act.

If you require any further Information or clarification, kindly contact the Information Officer.

Thank you for your Co-operation.

With kind regards,



**Pieter Uys**  
**Information Officer of the Company**

## **ANNEXURE G: DATA OPERATOR PRIVACY POLICY NOTICE: PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013**

The Company's Data Operator Privacy Notice applies to all Data Operators who receive and process Personal Information on behalf of the Company and forms part of the agreements between Data Operator and the Company.

### **1. NOTIFICATION**

- The Data Operator must immediately inform the Company in writing of any requests for Personal Information received from the Company's employees, clients, or any Third-Party.
- The Data Operator must notify the Company immediately in writing of any subpoena or other Judicial or Administrative Order by a government authority, seeking access to or disclosure of Personal Information.
- If the Data Operator becomes aware of any Information Security Incident, the Data Operator must, within 24 hours after becoming aware of the Incident, notify the Company's Information Officer, in writing.
- The Data Operator must specify the extent to which Personal Information was reasonably believed to have been compromised or disclosed.
- The Data Operator must investigate the Information Security Incident, preserve all documents, Personal Information and other Information related to the Information Security Incident.
- The Data Operator must provide the Company with an Incident Report.
- The Data Operator must cooperate with the Company.
- At the Company's request the Data Operator must cooperate with law enforcement, regulatory officials, credit reporting companies, and credit card associations investigating an Information Security Incident.
- The Company will make the final decision on notifying the Company's clients, employees, service providers and the public of an Information Security Incident.
- The Data Operator will be responsible for the costs associated with the performance of its obligations if the Information Security Incident did not result from the acts or omissions of the Company.

- The Data Operator must reimburse the Company for all Notification Related Costs incurred by the Company in connection with any such Information Security Incident.
- The Company will be responsible for the Data Operators' reasonable costs and expenses associated with the performance of its obligations if the Information Security Incident resulted from the acts or omissions of the Company.

## **2. COMPLIANCE WITH PRIVACY AND INFORMATION SECURITY REQUIREMENTS.**

- The Data Operator must comply with all privacy laws as they relate to Personal Information.
- The Data Operator confirms that no applicable law, or Information Security enforcement action, investigation, litigation, or claim prohibits the Data Operator from fulfilling its obligations under the Agreement with the Company.
- The Data Operator shall enter any further privacy, Information security, Personal Information Transfer or Personal Information Processing Agreement requested by the Company for purposes of compliance with applicable privacy laws.

## **3. PERSONAL INFORMATION SAFEGUARDS**

- The Data Operator must maintain and implement a comprehensive written Information Security Programme that complies with applicable privacy laws, including POPIA.
- The Data Operator's Information Security Programme must include administrative, technical, physical, organisational, and operational safeguards and security measures to:
  - Ensure the security and confidentiality of Personal Information.
  - Protect against any anticipated threats or hazards to the security and integrity of Personal Information.
  - Protect against any Information Security Incident.
  - Encourage timely internal reporting of Information Security Incidents.

- Facilitate appropriate response by the Data Operator to Information Security Incidents.
- The Data Operator's Information Security Policies shall provide for:
  - Regular assessment of the risks to the security of Personal Information and systems used by the Data Operator to Process Personal Information.
  - Identification of internal and external threats that could result in an Information Security Incident.
  - Assessment of the potential damage of such threats, considering the sensitivity of such Personal Information.
  - Assessment of Policies, Procedures, and Information Systems of the Data Operator, to control risks.
  - Protection against such risks.
- If the processing by the Data Operator, involves the transmission of the Personal Information over a network, the Data Operator must protect the Personal Information against the risks of such a transmission.
- The Data Operator must exercise supervision over its employees to maintain the privacy, confidentiality, and security of Personal Information.
- The Data Operator must provide training, regarding the privacy, confidentiality, and Information security requirements, to its employees who have access to Personal Information.
- Upon the expiration or termination of the Agreement, the Data Operator shall return to the Company every original and copy in every media of all Personal Information in the Data Operator's possession.
- If the law does not permit the Data Operator to deliver the Personal Information, the Data Operator warrants that it shall ensure the protection and confidentiality of the Personal Information and that it shall not use or disclose any Personal Information.

**4. RIGHT TO MONITOR**

The Company shall have the right to monitor the Data Operator's compliance with its Policies. The Data Operator shall deal promptly with any enquiries from the Company relating to the Processing of Personal Information subject to the Company's Policies.

**5. CHANGES IN THIS NOTIFICATION**

The Company reserves the right to amend, alter and terminate this Notification at any time.

A handwritten signature in black ink, appearing to be 'Pieter Uys', is written over a horizontal line.

**Pieter Uys**  
**Information Officer**



**ANNEXURE H: DATA OPERATOR INFORMATION PROCESSING AGREEMENT**

This Information Processing Agreement (this "Agreement") is entered into as of the \_\_\_\_ day of \_\_\_\_\_, 20\_\_\_\_ (the "Effective Date") by and between

The "Company":

Company Name:	Kaimara (Pty) Ltd
Company Registration Number:	2018/419858/07
VAT Registration Number	454 025 3848
Physical Address:	309 Brooks Street, Menlo Park, 0181
Postal Address:	309 Brooks Street, Menlo Park, 0181
Company Telephone Number:	+27 82 448 9662
Name of Information Officer:	Pieter Uys
e-mail Address of Information Officer:	<a href="mailto:pieter@kaimara.co.za">pieter@kaimara.co.za</a>

and

The "Data Operator":

Data Operator Name:	
Data Operator Registration Number:	
Physical Address:	

- Whereas the Company is required to adhere to the provisions of POPIA.
- Whereas the Data Operator collects, transmits, stores, or processes the Company Personal Information (as defined below).
- Whereas the Data Operator could impact the security and confidentiality of the Company Personal Information in the performance of the services it provides to the Company.

For purposes of this Agreement, the following terms have been defined:

- a) *“Main Agreement”* means the Agreement entered between the Company and the Data Operator in which the Data Operator provides products or services to the Company.
- b) *“POPIA” or “the POPI Act”* means the Protection of Personal Information Act, No. 4 of 2013, as amended.
- c) *“Security Incident”* means any unauthorised access, destruction, loss, alteration, disclosure, or any other unlawful forms of processing of the Company’s Personal Information.
- d) The *“Company”* means KAIMARA Pty Ltd
- e) *“Company Personal Information”* means any Personal Information which is provided to the Data Operator by the Company, or the Data Operator is required to process the Personal Information.
- f) The terms *“Data Subject”, “Personal Information”, “Processing”* and *“Regulator”* shall have the same meaning as in the POPIA.

***It is agreed that:***

1. The Data Operator will only process the Company Personal Information for the purposes or on the specific written instructions of the Company.
2. The Data Operator will comply with POPIA and not cause the Company to breach any obligation under POPIA.
3. The Data Operator will:
  - Process the Company Personal Information only with the knowledge or authorisation of the Company.

- Treat the Company Personal Information as confidential and shall not share, transfer, disclose or otherwise provide access to the Company Personal Information to any Third-Party.
4. The Data Operator will limit access to the Company Personal Information only to those employees to whom access is necessary to perform their role and then only on a need-to-know basis. The Data Operator will ensure that such employees:
    - i) Are subject to confidentiality obligations.
    - ii) Comply with this Agreement.
    - iii) Are appropriately reliable, qualified, and trained in relation to their processing of the Company Personal Information.
  5. The Data Operator will not use any Third-Party for the processing of the Company Personal Information.
  6. The Data Operator shall not cause or permit any of the Company Personal Information to be transferred outside the Republic of South Africa without the prior written consent of the Company.
  7. The Data Operator agrees that the Data Operator is responsible for the security and confidentiality of the Company Personal Information that it stores, transmits, or otherwise processes.
  8. The Data Operator undertakes and warrants that it will secure the integrity and confidentiality of the Company Personal Information by taking appropriate, reasonable technical and organisational measures to prevent:
    - a) Loss of, or damage to, or unauthorised destruction of the Company Personal Information.
    - b) Unlawful access to, or processing of, the Company Personal Information.
  9. The Data Operator will take reasonable measures to:
    - Identify all reasonably foreseeable internal and external risks to the Company Personal Information.
    - Establish and maintain appropriate safeguards against the risks identified.

- Regularly verify that the safeguards are effectively implemented, including conducting security assessments consistent with best industry Company.
  - Ensure that the safeguards are continually updated in respect of new risks or deficiencies in previously implemented safeguards.
  - Notify the Company of the risks identified, and the safeguards established and implemented.
10. The Data Operator will comply with:
- a) Generally accepted information security Company's and processes.
  - b) Best industry Company's or, where applicable, specific industry or professional rules and regulations.
  - c) The Company's security and requirements as the Company may notify the Data Operator.
11. Upon the Company's request, the Data Operator will:
- a) Provide the Company with all information necessary to demonstrate compliance with the obligations set out in this Agreement.
  - b) Allow for audits, conducted by the Company to confirm compliance with POPIA and this Agreement, including that the Company Personal Information is securely transferred.
  - c) Assist the Company in taking measures to address Security Incidents, including measures to mitigate their possible adverse effects.
  - d) Assist the Company in responding to requests, communications and complaints from Data Subjects, the Regulator, or any other authority.
12. The Data Operator will immediately notify the Company in writing, on:
- Becoming aware, that a Security Incident has occurred including, the nature of the Security Incident, the number and categories of Data Subjects, the likely consequences of the Security Incident and any measure to be taken to address the Security Incident and to mitigate its possible adverse effects.
  - Receipt of any request for access to or correction or disclosure of the Company Personal Information.
  - Complaints or any other communication from a Data Subject and provide the Company with a copy thereof.

13. The Data Operator will provide the Company with a detailed list of the POPIA requirements it is responsible for, as well as the requirements where responsibility is shared between it and the Company.
14. If the Company determines that the Data Operator has committed a breach of this Agreement or POPIA, the Company may either:
  - Offer the Data Operator an opportunity to remedy the breach.
  - Immediately terminate this Agreement.
16. At the option of the Company, securely return to the Company or transfer to any replacement service provider (in the format required by the Company) all Company Personal Information, and securely delete any remaining copies.
17. The Data Operator indemnifies the Company and its directors, employees and agents harmless against any and all losses, liabilities, damages, claims, fines, penalties, costs and expenses (including legal fees) arising out of or in connection with a breach by the Data Operator (or any of its employees) of this Agreement, non-compliance with POPIA or any unauthorised access, disclosure, or use of any of the Company Personal Information in the possession or under the control of the Data Operator.
18. This Agreement may only be amended by a written Agreement executed by the Data Operator and the Company.
19. The Agreement shall be binding upon the parties and their respective successors.
20. The Data Operator acknowledges that this Agreement shall commence on the Effective Date and continue so long as the Data Operator provides services or until terminated, whichever occurs first in time.
21. Termination of this Agreement will not affect the provisions, which are intended to continue to apply after termination.
22. If there is any unresolved dispute between the parties arising out of or in connection with this Agreement, the parties agree first to attempt to resolve the dispute informally by negotiation, and as far as possible avoid any formal dispute resolution process.
23. If the dispute is not so resolved, it shall be submitted to and decided by arbitration in terms of the Arbitration Act, 42 of 1965.

Signed on behalf of the Company:

Signed at \_\_\_\_\_ on this \_\_\_\_\_ day of \_\_\_\_\_ 20\_\_\_\_\_

Company Representative Signature	Company Representative Full Name
Witness Signature	Witness Full Name

Signed on behalf of the Data Operator:

Signed at \_\_\_\_\_ on this \_\_\_\_\_ day of \_\_\_\_\_ 20\_\_\_\_\_

Data Operator Representative Signature	Data Operator Representative Full Name
Witness Signature	Witness Full Name

## **POLICIES**

### **Prohibition on the Processing of Special Personal Information**

Policy	Prohibition on the Processing of Special Personal Information
Document No.	POL PE

#### **1. Prohibition on Processing of Special Personal Information**

The Company will not process personal information, concerning –

- a) The religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or
- b) The criminal behaviour of a data subject to the extent that such information relates to –
  - I. The alleged commission by a data subject of any offence; or
  - II. Any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

#### **2. General Authorisation Concerning Special Personal Information**

The prohibition on processing of special personal information, as referred to in clause 1 of this policy, does not apply if -

- a) Processing is carried out with the consent of the data subject; or
- b) Processing is necessary for the establishment, exercise or defence of a right or obligation in law; or
- c) Processing is for historical, statistical or research purposes to the extent that –
  - I. The purpose serves a public interest and the processing is necessary for the purpose concerned; or
  - II. It appears to be impossible or would involve a disproportionate effort to ask for consent, and sufficient guarantees are provided to ensure that the processing does not adversely affect the individual privacy of the data subject to a disproportionate extent; or
- d) Information has deliberately been made public by the data subject.

## Prohibition on the Processing of Special Personal Information Regarding Data Subject's Religious or Philosophical Beliefs

Policy	Prohibition on the Processing of Special Personal Information Regarding Data Subject's Religious or Philosophical Beliefs
Document No.	POL PF

### 1. Prohibition on the Processing of Special Personal Information

This policy should be read together with *Policy PE* regarding the Prohibition on the Processing of Special Personal Information.

### 2. Authorisation concerning data subject's religious or philosophical beliefs

#### 2.1 The prohibition on processing personal information concerning a data subject's religious or philosophical beliefs, as referred to in *Policy PF* regarding the Prohibition on the Processing of Special Personal Information, does not apply if the processing is carried out by –

- a) Spiritual or religious organisations, or independent sections of those organisations if –
  - I. The information concerns data subjects belonging to those organisations; or
  - II. It is necessary to achieve their aims and principles;
- b) Institutions founded on religious or philosophical principles with respect to their members or employees or other persons belonging to the institution, if it is necessary to achieve their aims and principles; or
- c) Other institutions: Provided that the processing is necessary to protect the spiritual welfare of the data subjects, unless they have indicated that they object to the processing.

#### 2.2 In the cases referred to in clause 2.1(a), the prohibition does not apply to processing of personal information concerning the religion or philosophy of life of family members of the data subject, if

- a) The association concerned maintains regular contact with those family members in connection with its aims; and
- b) The family members have not objected in writing to the processing of special personal information.

#### 2.3 Personal information concerning a data subject's religious and philosophical beliefs may not be supplied to third parties without the consent of the data subject.



## Prohibition on the Processing of Special Personal Information Regarding Data Subject's Race or Ethnic Origin

Policy	Prohibition on the Processing of Special Personal Information Regarding Data Subject's Race or Ethnic Origin
Document No.	POL PG

### 1. Prohibition on the Processing of Special Personal Information

This policy should be read together with *Policy PE* regarding the Prohibition on the Processing of Special Personal Information.

### 2. Authorisation Concerning a Data Subject's Race or Ethnic Origin

#### 2.1 The prohibition on processing personal information concerning a data subject's race or ethnic origin, as referred to in *Policy PE* regarding the Prohibition on the Processing of Special Personal Information, does not apply if the processing is carried out to –

- a) Identify data subjects and only when this is essential for that purpose; and
- b) Comply with laws and other measures designed to protect or advance persons, or categories of persons, disadvantaged by unfair discrimination.

## Prohibition on the Processing of Special Personal Information Regarding Data Subject's Trade Union Membership

Policy	Prohibition on the Processing of Special Personal Information Regarding Data Subject's Trade Union Membership
Document No.	POL PH

1. Prohibition on the Processing of Special Personal Information  
This policy should be read together with *Policy PE* regarding the Prohibition on the Processing of Special Personal Information.
2. Authorisation Concerning a Data Subject's Trade Union Membership
  - 2.1 The prohibition on processing personal information concerning a data subject's trade union membership, as referred to in *Policy PE* regarding the Prohibition on the Processing of Special Personal Information, does not apply to the processing by the trade union to which the data subject belongs or the trade union federation to which that trade union belongs, if such processing is necessary to achieve the aims of the trade union federation.
  - 2.2 In cases referred to in clause 2.1, no personal information may be supplied to third parties without the consent of the data subject.

## Prohibition on the Processing of Special Personal Information Regarding Data Subject's Political Persuasion

Policy	Prohibition on the Processing of Special Personal Information Regarding Data Subject's Political Persuasion
Document No.	POL PI

### 1. Prohibition on the Processing of Special Personal Information

This policy should be read together with *Policy PE* regarding the Prohibition on the Processing of Special Personal Information.

### 2. Authorisation Concerning Data Subject's Political Persuasion

2.1 The prohibition on processing personal information concerning a data subject's political persuasion, as referred to in *Policy PE* regarding the Prohibition on the Processing of Special Personal Information, does not apply to processing by or for an institution, founded on political principles, of the personal information of –

- a) Its members, employees or other persons belonging to the institution, if such processing is necessary to achieve the aims or principles of the institution; or
- b) Participating in the activities of, or engaging in the recruitment of members for or canvassing supporters or voters for, a political party.

2.2 In the cases referred to in clause 2.1, no personal information may be supplied to third parties without the consent of the data subject.

## Prohibition on the Processing of Special Personal Information Regarding Data Subject's Health or Sex Life

Policy	Prohibition on the Processing of Special Personal Information Regarding Data Subject's Health or Sex Life
Document No.	POL PJ

### 1. Prohibition on the Processing of Special Personal Information

This policy should be read together with *Policy PE* regarding the Prohibition on the Processing of Special Personal Information.

### 2. Authorisation Concerning Data Subject's Health or Sex Life

#### 2.1 The prohibition on processing personal information concerning a data subject's health or sex life, as referred to in *Policy PE* regarding the Prohibition on the Processing of Special Personal Information, does not apply to the processing by –

- a) Medical professionals, healthcare institutions or facilities or social services, if such processing is necessary for the proper treatment and care of the data subject, or for the administration of the institution or professional Company concerned;
- b) Insurance companies, medical schemes, medical scheme administrators and managed healthcare organisations, if such processing is necessary for–
  - I. Assessing the risk to be insured by the insurance Company or covered by the medical scheme and the data subject has not objected to the processing; or
  - II. The performance of an insurance or medical scheme agreement; or
  - III. The enforcement of any contractual rights and obligations;
- c) Schools, if such processing is necessary to provide special support for pupils or making special arrangements in connection with their health or sex life;
- d) Any public or private body managing the care of a child if such processing is necessary for the performance of their lawful duties;
- e) Any public body, if such processing is necessary in connection with the implementation of prison sentences or detention measures; or

- f) Administrative bodies, pension funds, employers or institutions working for them, if such processing is necessary for –
  - I. The implementation of the provisions of laws, pension regulations or collective agreements which create rights dependent on the health or sex life of the data subject; or
  - II. The reintegration of or support for workers or persons entitled to benefit in connection with sickness or work incapacity.
- 2.2 In cases referred to in clause 2.1, the information may only be processed by the Company subject to an obligation of confidentiality by virtue of office, employment, profession or legal provision, or established by a written agreement between the Company and the data subject.
- 2.3 Where the Company is permitted to process information concerning a data subject's health or sex life in terms of this policy and is not subject to an obligation of confidentiality as referred to in clause 2.2, it must treat the information as confidential, unless the Company is required by law or in connection with its duties to communicate the information to other parties who are authorised to process such information in accordance with clause 2.1.
- 2.4 Personal information concerning inherited characteristics may not be processed in respect of a data subject from whom the information concerned has been obtained, unless –
  - a) A serious medical interest prevails; or
  - b) The processing is necessary for historical, statistical or research activity.

## Prohibition on the Processing of Special Personal Information Regarding Data Subject's Criminal Behaviour or Biometric Information

Policy	Prohibition on the Processing of Special Personal Information Regarding Data Subject's Criminal Behaviour or Biometric Information
Document No.	POL PK

1. Prohibition on the Processing of Special Personal Information  
This policy should be read together with *Policy PE* regarding the Prohibition on the Processing of Special Personal Information.
2. Authorisation Concerning Data Subject's Criminal Behaviour or Biometric Information
  - 2.1 The prohibition on processing personal information concerning a data subject's criminal behaviour or biometric information, as referred to in *Policy PE* regarding the Prohibition on the Processing of Special Personal Information, does not apply if the processing is carried out by bodies charged by law with applying criminal law or where the Company obtained that information in accordance with the law.
  - 2.2 The processing of information regarding personnel in the service of the Company must take place in accordance with the rules established in compliance with labour legislation.

## Prohibition on the Processing of Personal Information of Children

Policy	Prohibition on the Processing of Personal Information of Children
Document No.	POL PL

### 1. Prohibition on the Processing of Personal Information of Children

The Company may not process any personal information of children, unless as allowed for in clause 2 of this policy.

### 2. General Authorisation Concerning Personal Information of Children

The processing of personal information of children will only be allowed in the following circumstances:

- a) If it is carried out with the prior consent of a competent person;
- b) If it is necessary for the establishment, exercise or defence of a right or obligation in law;
- c) If it is necessary to comply with an obligation of international public law;
- d) If it is for historical, statistical or research purposes to the extent that –
  - I. The purpose serves a public interest and the processing is necessary for the purpose concerned; or
  - II. It appears to be impossible or would involve disproportionate effort to ask for consent; or
  - III. sufficient guarantees are provided for to ensure that the processing does not adversely affect the individual privacy of the child to a disproportionate extent; or
- e) Where the personal information has deliberately been made public by the child with the consent of a competent person.

## Processing Subject to Prior Authorisation

Policy	Processing Subject to Prior Authorisation
Document No.	POL PM

1. Processing Subject to Prior Authorisation
  - 1.1 The Company must obtain prior authorisation from the Regulator, prior to any processing if the Company plans to –
    - a) Process unique identifiers of data subjects –
      - I. For a purpose other than the one for which the identifier was specifically intended at collection; and
      - II. With the aim of linking the information together with information processed by other responsible parties;
    - b) Process information on criminal behaviour or on unlawful or objectionable conduct on behalf of third parties;
    - c) Process information for the purpose of credit reporting; or
    - d) Transfer special personal information or the 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.
  - 1.2 The Company will only have to obtain the prior authorisation once and not each time that personal information is received or processed, except where the processing departs from that which has been authorised by the Regulator.
2. The Company to Notify the Regulator if Processing is Subject to Prior Authorisation
  - 2.1 The Company must notify the Regulator when processing personal information referred to in clause 1.1 of this policy.
  - 2.2 The Company may not carry out information processing that has been notified to the Regulator until the Regulator has completed its investigation or until they have received notice that a more detailed investigation will not be conducted.



## Direct Marketing by Means of Unsolicited Electronic Communications

Policy	Direct Marketing by Means of Unsolicited Electronic Communications
Document No.	POL PN

1. Direct Marketing by means of Unsolicited Electronic Communications
  - 1.1 The processing of personal information of a data subject for the purpose of direct marketing by means of any form of electronic communication, including automatic calling machines, facsimile machines, SMSs or e-mail is prohibited unless the data subject –
    - a) Has given his, her or its consent in writing to the processing; or
    - b) Is a customer of the Company.
  - 1.2 The Company may approach the data subject –
    - a) Whose consent is required; and
    - b) Who has not previously withheld such consent, only once in order to request the consent of that data subject in the prescribed manner and form.
  - 1.3 The Company may only process the personal information of a data subject who is a customer of the Company –
    - a) If the Company has obtained the contact details of the data subject in the context of the sale of a product or service provided;
    - b) For the purpose of direct marketing of the Company's own similar products or services; and
    - c) If the data subject has been given a reasonable opportunity to object, free of charge and in a manner free of unnecessary formality, to such use of his, her or its electronic details –
      - I. At the time when the information was collected; and
      - II. On the occasion of each communication with the data subject for the purpose of marketing if the data subject has not initially refused such use.
  - 1.4 Any communication for direct marketing must contain –
    - a) Details of the identity of the sender or the person on whose behalf the communication has been sent; and

- b) An address or other contact details to which the recipient may send a request that such communications cease.

## Transborder Information Flows

Policy	Transborder Information Flows
Document No.	POL PO

### 1. Transfer of Personal Information outside the Republic

The Company may not transfer personal information about a data subject to a third party who is in a foreign country unless –

- a) The third party who is the recipient of the information is subject to a law, binding corporate rules or binding agreement which provide an adequate level of protection that –
  - I. Effectively upholds principles for reasonable processing of the information that are substantially similar to the conditions for the lawful processing of personal information relating to a data subject who is a natural person, and where applicable, a juristic person; and
  - II. Includes provisions, that are substantially similar to this policy, relating to the further transfer of personal information from the recipient to third parties who are in a foreign country;
- b) The data subject consents to the transfer;
- c) The transfer is necessary for the performance of a contract between the data subject and the Company, or for the implementation of pre-contractual measures taken in response to the data subject's request;
- d) The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the Company and a third party; or
- e) The transfer is for the benefit of the data subject, and –
  - I. It is not reasonably practicable to obtain the consent of the data subject to that transfer; and
  - II. If it were reasonably practicable to obtain such consent, the data subject would be likely to give it.

## Additional Policies:

### Acceptable Use Policy

Policy	Acceptable Use Policy
Document No.	POL APA

#### 1. **PURPOSE**

- 1.1 The purpose of this policy is to direct all employees of the Company in the acceptable use and security of the Company's Internet Facilities. These standards contain directions for employees, indicating both acceptable and unacceptable Internet use with the aim of controlling employee behaviour and actions that contribute to the Company's Internet risks, while maximizing the benefits gained by the Company through Internet usage. As the software, hardware and computer network is the property of the Company it reserves the right to keep the Company and its systems secure through monitoring electronic information and regular checks on the system.

#### 2. **ROLES AND RESPONSIBILITIES**

- 2.1 The Company's Management will establish a periodic reporting requirement to measure the compliance and effectiveness of this policy.
- 2.2 The Company's Management is responsible for implementing the requirements of this policy, or documenting non-compliance via the method described under exception handling.
- 2.3 The Company's Managers, in cooperation with the Information Officer, are required to train employees on policy and document issues with Policy compliance.
- 2.4 All of the Company's employees are required to read and acknowledge the reading of this policy by signing it.

#### 3. **POLICY DIRECTIVES**

##### Part I - Management Requirements

1. The Company will establish formal Standards and Processes to support the on-going development and maintenance of the Company's Acceptable Use Policy.
2. The Company's Director(s) and Management will commit to the on-going training and education of the Company's staff responsible for the administration and/or maintenance and/or use of the Company's Internet facilities.
3. The Company's Director(s) and Managers will establish a formal review cycle for all Acceptable Use initiatives.

4. Any security issues discovered will be reported to the Information Officer or his Deputy Information Officers.

## Part II – Ownership

Electronic files created, sent, received, or stored on Information Resources owned, leased, administered, or otherwise under the custody and control of the Company are the property of the Company and employee use of these files is neither personal nor private. The Information Officer may access all such files at any time without knowledge of the user or owner. The Company's management reserves the right to monitor and/or log all employee use of the Company's Information Resources with or without prior notice.

## Part III – Acceptable Use Requirements

1. Employees will only be given sufficient rights to all systems to enable them to perform their job function. User rights will be kept to a minimum at all times.
2. Employees must report any weaknesses in the Company's computer security to the appropriate security staff. Weaknesses in computer security include unexpected software or system behaviour, which may result in unintentional disclosure of information or exposure to security threats.
3. Employees must report any incidents of possible misuse or violation of this Acceptable Use Policy to the Information Officer.
4. Employees must not attempt to access any data, documents, email correspondence, and programs contained on the Company's systems for which they do not have authorization.
5. Employees must not attempt any access penetration tests, any investigations or perform any other activities to compromise the access controls of the Company's computing facilities, unless there is a demonstrated Company requirement to do so and the Company's Manager has approved of such activities and the conditions under which it will apply in advance in writing.
6. Systems administrators and authorized users must not divulge remote connection modem phone numbers or other access points to the Company's computer resources to anyone without proper authorization in writing.
7. Employees must not share their account(s), passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), or similar information or devices used for identification and authorization purposes.
8. Employees must not make unauthorized copies of copyrighted software or software owned by the Company.

9. Employees must not use non-standard shareware or freeware software without the approval from Management.
10. Employees must not purposely engage in activity that may harass, threaten or abuse others or intentionally access, create, store or transmit material that the Company may deem to be offensive, indecent or obscene, or that is illegal in terms of applicable legislation.
11. Employees must not engage in activity that may degrade the performance of Information Resources; deprive an authorized user access to the Company's resources; obtain extra resources beyond those allocated; or circumvent the Company's computer security measures.
12. Employees must not download, install or run security programs or utilities such as password cracking programs, packet sniffers, or port scanners that reveal or exploit weaknesses in the security of the Company's computer resources unless approved by Information Officer.
13. The Company's Information Resources must not be used for personal benefit, political activity, unsolicited advertising, unauthorized fund raising, or for the solicitation of performance of any activity that is prohibited by relevant legislation.
14. Access to the Internet from home based computers or computers owned by the Company, must adhere to all the policies. Employees must not allow family members or other non-employees to access non-public accessible computer systems of the Company.
15. Employees must not attempt to change the configuration of desktop computers and notebooks. All configuration changes must be handled by the IT department, for example upgrading operating systems, changing Windows settings, installing new software or systems, and installing modems, memory or storage upgrades.
16. In particular, the Company's Internet facilities may not be used for any of the following:
  - Communications in connection with the personal Company interests of the user or the user's family.
  - Downloading, transmission, and possession of pornographic and sexually explicit materials.
  - Transmitting defamatory, slanderous, threatening and abusive messages, inflammatory statements, or any message that may be construed as such.

- Political or religious statements, foul language, or any other statements viewed as harassing others based on race, creed, colour, age, sex, national origin, disability or physical attributes are prohibited.
  - Unauthorized attempts to bypass or any attempt to circumvent any security mechanisms of computers connected to the Internet.
  - Propagating, sending, responding to, redirecting, forwarding, or otherwise participating in chain letters or junk e-mail.
  - The alteration, destruction, or infringement of the privacy of other employees' computer-based information residing on the Internet and e-mail systems.
  - Playing computer games or engaging in any other form of entertainment or sporting activities during Company hours.
  - Any communications or activity, which could harm the good name and reputation of the Company.
17. Employees of the Company may not send or publish confidential and private material of the Company (internal memos, policies, etc.) on any publicly accessible or external Internet computer of the Company unless the owner of the information has first approved the publication of these materials.
18. Employees should not transmit confidential information, information of the Company, copyrighted materials, or any trade secrets of the Company over any public computer system or network unless properly protected through encryption methods.
19. Any security issues discovered will be reported to the Information Officer or his Deputy Information Officers.

#### Part IV – Incidental Use

1. Incidental personal use of electronic mail, Internet access, fax machines, printers, and copiers is restricted to the Company's approved users only and does not include family members or others not affiliated with the Company.
2. Occasional private use of the Company's Internet facilities are allowed under the following conditions:
  - Occasional and very short personal email communications by users are acceptable provided that they do not interfere with the users work and comply with the guidelines of this policy at all times.

If the user is not sure whether a personal communication complies with the requirements of this policy, the prior authorization of the user's superior must be obtained before such messages are sent.

- Personal use of the Company's Internet facilities must be kept to a minimum and in any event must not exceed 2 hours per week per user during office hours and 4 hours (1 hour at a time) per week after hours. Personal usage must not interfere with the user's work and such usage must comply with the requirements of this policy at all times.
- 3. Incidental use must not result in direct costs to the Company, cause legal action against, or cause embarrassment to the Company.
- 4. Incidental use must not interfere with the normal performance of an employee's work duties.
- 5. Storage of personal email messages, voice messages, files and documents within the Company's computer resources must be nominal.
- 6. The Company's Management will resolve incidental use questions and issues using these guidelines in collaboration with the Information Officer, HR Manager and the Line Manager/Supervisor.

#### 4. **ENFORCEMENT, AUDITING AND REPORTING**

1. Violation of this policy may result in disciplinary action that may include termination for employees and temporaries; termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers. Additionally, individuals are subject to loss of the Company's Information Resources access privileges, civil, and criminal prosecution.
2. The Company's Management is responsible for the periodic auditing and reporting of compliance with this policy. The Company's Information Officer will be responsible for defining the format and frequency of the reporting requirements and communicating those requirements, in writing, to the Company's Director(s).
3. Exceptions to this policy will be considered only when the requested exception is submitted in writing to the Information Officer.
4. Any employee may, at any time, anonymously report policy violations to the Information Officer.



## E-mail Policy

Policy	E-mail Policy
Document No.	POL APB

### 1. **INTRODUCTION**

The Company provides employees with electronic communication tools, including an e-mail system. This email policy, which governs employee use of the Company e-mail system, applies to e-mail use at the Company's premises and district offices, as well as remote locations, including, but not limited to, employee homes, airports, hotels, and client and supplier offices. The Company's e-mail rules and policies apply to full-time employees, part-time employees, independent contractors, interns, consultants, suppliers, clients, and other third parties. Any employee who violates the Company's e-mail rules and policies is subject to disciplinary action, up to and including termination.

### 2. **E-mail EXISTS FOR COMPANY PUPOSES**

The Company allows e-mail access primarily for Company purposes. Employees may use the Company's e-mail system for personal use only in accordance with the Company's policies.

### 3. **E-mail MONITORING**

The Company reserves the right to monitor, inspect, copy, review, and store any and all employee's e-mail use at any time and without prior notice. In addition, the Company may monitor, inspect, copy, review, and store any files, information, software, and other content created, sent, received, downloaded, uploaded, accessed, or stored through the Company's e-mail system. The Company reserves the right to disclose e-mail information and images to regulators, courts, law enforcement agencies, and other third parties without the employee's consent.

### 4. **BANNED ACTIVITIES**

Employees are prohibited from using e-mail to engage in activities or transmit content that is harassing, discriminatory, menacing, threatening, obscene, defamatory, or in any way objectionable or offensive.

### 5. **Employees Are Prohibited From Using E-mail to:**

- 5.1 Send, receive, solicit, print, copy, or reply to text, images, or jokes that disparage others based on their race, religion, colour, gender, sex, sexual orientation, national origin, veteran status, disability, ancestry, or age.

- 5.2 Send, receive, solicit, print, copy, or reply to messages that are disparaging or defamatory.
- 5.3 Spread gossip, rumours, or innuendos about employees, clients, suppliers, or other outside parties.
- 5.4 Send, receive, solicit, print, copy, or reply to sexually oriented messages or images.
- 5.5 Send, receive, solicit, print, copy, or reply to messages or images that contain foul, obscene, disrespectful, or adult-oriented language.
- 5.6 Send, receive, solicit, print, copy, or reply to messages or images that are intended to alarm others, embarrass the Company, negatively impact employee productivity, or harm employee morale.

## **6. CONFIDENTIAL, PROPRIETARY AND PI MUST BE PROTECTED**

Unless authorized to do so, employees are prohibited from using e-mail to transmit confidential information to outside parties. Employees may not access, send, receive, solicit, print, copy, or reply to confidential or proprietary information about the Company, its employees, clients, suppliers, and other Company associates unless it is in the best interest of the Company to do so. Confidential information includes, but is not limited to, client lists, credit card numbers, identification numbers, employee performance reviews, salary details, trade secrets, passwords, and information that could embarrass the Company and its employees if the information were disclosed to the public.

## **7. COMPANY RECORD RETENTION**

E-mail messages are written Company records and are subject to the Company's rules and policies for retaining and deleting Company records. Please refer to the Company's Data Retention Policy for more information.

## **8. INFORMATION EXCHANGE AND INTERNET TRANSACTIONS**

- 8.1 All messages communicated on the Company's Internet and e-mail system must contain the employee's name.  
  
No e-mail or any other electronic communication may be sent which hides the identity of the sender or represents the sender as someone else. All emails sent must include the email signature of the sender.
- 8.2 Emails with attachments sent by employees may not exceed the limit as prescribed by the Information Officer.
- 8.3 The disclaimer as prescribed by the IT department must be used at the end of all email messages

## **9. VIOLATIONS**

These guidelines are intended to provide the Company's employees with general examples of acceptable and unacceptable uses of the Company's e-mail system. A violation of this policy may result in disciplinary action up to and including termination.

## Handheld & Mobile Device Policy

Policy	Handheld & Mobile Device Policy
Document No.	POL APC

### 1. **PURPOSE**

This policy establishes rules for the proper use of handheld devices in the Company in order to protect the confidentiality of sensitive data, the integrity of data and applications, and the availability of services at the Company, protecting both handheld devices and their users, as well as corporate assets (confidentiality and integrity) and continuity of the Company.

### 2. **SCOPE OF APPLICATION AND OBLIGATIONS**

This policy applies to all employees, consultants, vendors, contractors, students, and others using Company or private mobile handheld devices on any premises occupied by the Company. Adherence to these requirements and the security policies derived from them and implementation of provisions is binding across the whole of the Company, its subsidiaries and majority holdings. Wilful or negligent infringement of the policies jeopardizes the interests of the Company and will result in disciplinary, employment, and/or legal sanctions. In the case of the latter the relevant line managers and where applicable legal services shall bear responsibility. These requirements and the security policies derived from them and implementation provisions also apply to all suppliers of the Company. They shall be contractually bound to adhere to the security directives. If a contractual partner is not prepared to adhere to the provisions, he must be bound in writing to assume any resulting consequential damage.

### 3. **ROLES & RESPONSIBILITY**

- 3.1 The IT department must ensure that all employees using devices falling into the category of “handheld devices” have acknowledged this security policy and the associated procedures before they are allowed to use corporate services using handheld devices.
- 3.2 The IT department must ensure that handheld devices and their users comply with this security policy and all security policies as stipulated by the Company.
- 3.3 Any employee found to have violated this policy is subject to disciplinary action, up to and including termination.
- 3.4 In a general sense, all users are required to use their common sense in order to act in the best interest of the Company, its assets and its services.
- 3.5 In case of doubt, users must contact the IT department to clarify a given situation.

- 3.6 Users of handheld devices must diligently protect such devices from loss and disclosure of private information belonging to or maintained by the Company.
- 3.7 Before connecting a mobile handheld device to the network at the Company, users must ensure it is on the list of approved devices issued by the IT department.
- 3.8 The IT department must be notified immediately upon suspicion of a security incident, especially when a mobile device may have been lost or stolen.
- 3.9 The cost of any item beyond the standard authorized equipment is the responsibility of the employee.

#### 4. **EXCEPTIONS TO HANDHELD SECURITY POLICY**

Requests for an exception to this policy must be submitted to and approved by the Information Officer.

#### 5. **USE OF PRIVATE HANDHELD DEVICES**

The Information Officer must define whether private handhelds are authorised to connect to the Company's networks.

##### 5.1 Private handhelds are not authorised:

- In highly restricted facilities, private handheld devices must be prohibited. In that case, mobile devices must be collected prior to the user's entrance into the facility.
- Private handhelds are authorised in offices, but are not allowed to connect to internal networks.
- Private handhelds must not connect to the Company's networks and access corporate information. This includes synchronization with a workstation connected to the internal networks. The Company's networks must be protected accordingly using network access control mechanisms and must not grant access to any corporate information to unregistered devices.

##### 5.2 Private handhelds are authorised:

- Any non-Company-owned (private) device able to connect to the Company's network must first be approved by the IT department.
- If allowed, privately-owned handheld devices must comply with this policy and must be inventoried along with corporate handheld devices, but identified as private. This is in order to prevent theft of corporate data with unmanaged handhelds.

## 6. **IT DEPARTMENT ROLES AND RESPONSIBILITIES**

- 6.1 The IT department is responsible for the mobile handheld device policy at the Company and shall conduct a risk analysis to document safeguards for each device type to be used on the network or on equipment owned by the Company.
- 6.2 This policy should be reviewed on an annual basis by the Information Officer and IT department of the Company, taking into account changes according to new services available, new capabilities of devices, changes in corporate backend servers, and new threats to mobile devices.
- 6.3 The IT department is responsible for developing procedures for implementing this policy.
- 6.4 The IT department maintains a list of approved mobile handheld devices and makes the list available on the intranet.
- 6.5 The IT department maintains a list of allowed and unauthorised applications.

## 7. **USER AWARENESS TRAINING**

- 7.1 Users must be trained in order to ensure the proper use of devices and resources of the Company. A focus on applications and basic security features of the Company is mandatory.
- 7.2 The following list is not exhaustive, but contains crucial points that must be addressed during the initial training:
  - Review of policies
  - Procedure implementation
  - Password protection
  - How to deal with social engineering attacks
  - Proper protection of devices
  - Locking the device
  - Preventing the use of systems by unauthorised users
  - Protecting devices from loss or theft
  - Ensuring the information on a handheld device is absolutely necessary
  - Ensuring the information on a handheld device is also stored on the Company's network where it is regularly backed up
  - How to encrypt sensitive information
  - User awareness of changes in technologies and security policies should be regularly tested.

## 8. **INVENTORY OF MOBILE DEVICES**

- 8.1 The IT department must keep inventory of handhelds in use in the Company, using associating owner names and identity for network access control.
- 8.2 The inventory must take into account at least but not limited to the following list of identifiers:
- Device name
  - Owner's ID
  - Device serial number
  - Device IMEI
  - Device's MAC address
  - Owner's ID (user)
  - User's MSISDN
  - Device capabilities (Bluetooth, IrDA, Camera, etc.)
  - Supplementary accessories provided

## 9. **AUTHORISED SERVICES AND APPLICATIONS**

- 9.1 Only approved third party applications may be installed on handhelds. The approved list can be obtained by contacting the IT department.
- 9.2 In the event that a desired application is not on the list, a request can be submitted to the IT department. If the program meets internal testing requirements of stability and security, it will be added and at that point it may be installed.

## 10. **FORBIDDEN DEVICES**

- 10.1 The IT department must provide a list of unauthorised applications and communicate it to the users.
- 10.2 The list of unauthorised applications must remain available to the users via the intranet.
- 10.3 The following services might be disabled according to the Company's risk analysis in order to prevent information disclosure or data leakage:
- Peer-to-peer services (e.g. Skype);
  - MMS messages;
  - Instant messaging;
  - Camera;
  - Third-party applications;

- Any type of tunnelling application that does not allow filtering of the content of communications, except the approved VPN solution.

## 11. **AUTHORISED ACTIONS**

11.1 Users must not modify security configurations without request to and approval by the IT department. Failure to comply with this rule will engage disciplinary procedures.

11.2 Unauthorised actions:

- Installing and/or using unauthorised applications or services;
- Removing root certificates from certificate stores;
- Conducting any careless actions leading to an interruption or service;
- Disabling security features.

## 12. **UNCOVERED ISSUES**

All issues that are not covered by this security policy must be brought to the attention of the Information Officer or IT department of the Company, which will treat them on a case-by-case basis.



## Access Control Policy

Policy	Access Control Policy
Document No.	POL APD

### 1. **PURPOSE**

This policy establishes the guidelines for managing user access to information of the Company. The purpose is to ensure the necessary user access controls are in place for controlling the actions, functions, applications, and operations of legitimate users. The aim is to protect the confidentiality, integrity, and availability of all the Company's information resources.

All managers of the Company's information resources will ensure that access to the Company's information is properly authorized and granted with correct access levels and privileges applied.

### 2.1 **OPERATIONAL DEFINITIONS**

2.1.1 "Authentication": Verification that the user's claimed identity is valid and is usually implemented through a user password at logon.

2.1.2 "Discretionary User Access": The ability to manipulate data using custom or general-purpose programs. The only information logged for discretionary control mechanisms is the type of data accessed and at what level of authority.

2.1.3 "Identification": The act of a user professing an identity to a system, usually in the form of a logon to the system.

2.1.4 "Non-discretionary User Access": The access obtained in the process of specific Company transactions that affect information in a predefined way. For example, the Company's deployment specialists need to access participant information to make travel arrangements, but may not need the ability to change any existing information.

2.1.5 "Password": An arrangement of characters entered by a system user to substantiate their identity, authority, and access rights to an information system they wish to use.

2.1.6 "Privilege": The level of user authority or permission to access information resources. Privileges can be established at the folder, file, or application levels, or for other conditions as applicable.

2.1.7 "Special User Access Privileges": Privileges that allow users to perform specialized tasks that require broad capabilities. For example changing control functions such as: access control, logging, and violation detection, require special access privileges.

2.1.8 "User Account": An issued name with authority, granted to an individual to access a system or software application. System administrators, with proper

management approval, typically grant accounts. To access an account, a user needs to be authenticated, usually by providing a password.

- 2.1.9 “User Access Controls”: The rules and deployment of mechanisms, which control access in information resources, and physical access to premises.

## 2.2. User Accounts

The creation of a user account must be initiated through a request to the Information Officer who is authorised to approve access to the specified resources.

## 2.3. Account Management

The Company’s IT department manages user accounts for the Company’s systems. Records of processed and denied requests for creation of user accounts must be kept for auditing purposes. Records will be retained for one year, unless otherwise specified in the Data Retention Policy.

## 2.4. User Accounts Characteristics

All employee user accounts must be unique, and traceable to the assigned user. The IT department of the Company will take appropriate measures to protect the privacy of user information associated with user accounts. The use of group accounts and group passwords is not allowed, unless specifically approved by the Director(s) of the Company.

## 2.5. Password Reset

The IT department of the Company will establish a procedure for verifying a user’s identity prior to resetting their password.

## 2.6. User Account Privileges

Users will be granted the minimum access required to perform their specific tasks. Granting access levels to resources shall be based on the principle of least privilege, job responsibilities, and separation of duties. The level of minimum access requires the recommendation of the user’s manager, and the evaluation of the Information Officer. The Information Officer has final determination as to the level of a user’s access for their system.

## 2.7. Inactive Accounts

Accounts will be disabled after 30 days of inactivity. Users planning to deploy to field operating locations or to be away from the office for other approved periods of extended absence should be coordinated with the IT department in order to ensure proper disposition of the account.

## 2.8. Temporary User Accounts

All requests for temporary user accounts shall provide an expiration date to be applied at the time the account is created.

Applications for temporary user accounts should be submitted for approval to the IT department.

## 2.9 Password Characteristics

All passwords must be constructed using the following characteristics: alphanumeric characters, with a mixture of letters, numbers and special characters. The IT department will implement appropriate procedures and technology to enforce this requirement.

## 2.10 Automatic Logon

The use of automatic logon software to circumvent password entry shall not be allowed, except with specific approval from the Information Officer, for special tasks such as automated backups.

## 2.11 User Account and Password Safekeeping

Each individual assigned a user account and password is responsible for the actions taken under said account, and must not divulge that account information to any other person for any reason.

## 2.12 Management of User Accounts

Management access to user accounts will be limited to Company purposes only, such as during an emergency or contingency situation, cases of extended user absence, or user abuse of the Company's information resources. The IT department will establish procedures for providing their management with access to accounts assigned to a user within their department. These procedures will be coordinated with the Director(s) and Information Officer.

## 2.13 Transfers

Personnel transferring from one area of responsibility to another shall have their access accounts modified to reflect their new job responsibilities.

## 2.14 User Access Cancellation

The IT department will implement procedures to immediately cancel account access and physical access for users whose relationship with the Company has concluded, either on friendly or unfriendly terms.

## 2.15 User Session Time-out

User sessions will time-out after the prescribed period of inactivity has lapsed, unless otherwise specified as part of the system or application security plan. This includes user connections to the Internet, or to specific applications.

## 2.16 Remote Access Security

Access points for remote computing devices shall be configured using necessary identification and authentication technologies to meet security levels of physically connected computers.

## 2.17 New Information Systems

All new information systems acquired or developed by the IT department will incorporate access controls to properly protect the Company's information resources.

## 2.18 Sensitive Information Access

Individuals in positions with access to sensitive information will be screened for best suitability to the position. These individuals will be subject to the provisions of the Company's policies and procedures to protect and safeguard such information from unauthorised disclosure or access.

## 2.19 Temporary Access to Sensitive Resources

Temporary access to resources categorised as sensitive will be set with expiration dates where possible. The IT department will monitor temporary access to ensure activities comply with the intended purpose.

# 3. APPLICABILITY AND COMPLIANCE

This policy applies to all information resources, systems, and technology and to all users of these resources, systems and technology within the Company's operating environment or connected to the Company's information infrastructure.

# 4. RESPONSIBILITIES

## 4.1 The Company's Information Officer

The Information Officer will coordinate the implementation of this policy.

## 4.2 The Company's IT Department

The IT department will establish procedures to implement these requirements.

# 5. PROGRAM IMPLEMENTATION

The IT department will establish processes and procedures to implement this policy, and coordinate activities with the Information Officer.

## 5.1 User Access Administration

The Information Officer has primary management responsibility for administering user access to the Company's information resources.

## Physical Security Policy

Policy	Physical Security Policy
Document No.	POL APE

### 1. **PURPOSE**

All of the Company's premises that include computers and other types of information technology resources must be safeguarded against unlawful and unauthorized physical intrusion, as well as fire, flood and other physical threats. This includes but is not limited to; security doors, key entry areas, external doors that are locked from closing until opening of the building, locked and/or barred windows, security cameras, registration of visitors at entrances, security guards, and fire protection.

### 2. **SCOPE**

This policy addresses threats to critical IT resources that result from unauthorized access to facilities owned or leased by the Company, including offices, data centres and similar facilities that are used to house such resources.

### 3. **POLICY**

All information resource facilities must be physically protected in proportion to the criticality or importance of their function. Physical access procedures must be documented, and access to such facilities must be controlled. Access lists must be reviewed at least quarterly or more frequently depending on the nature of the systems that are being protected.

#### 3.1 Use of Secure Areas to Protect Data and Information

The Company must use physical methods to control access to information processing areas. These methods could include, but are not limited to, locked doors, secured cage areas, vaults, ID cards, and biometrics.

#### 3.2 Physical Access management to protect data and information

Access to facilities that holds critical IT infrastructure, systems and programs must follow the principle of least privilege access. Employees, including full and part-time staff, contractors and vendors' staff should be granted access only to facilities and systems that are necessary for the fulfilment of their job responsibilities.

The process for granting physical access to information resource facilities must include the approval of the Information Officer, or his or her deputy.

Access reviews must be conducted at least quarterly, or more frequently depending on the nature of the systems that are being protected.

Removal of individuals who no longer require access must then be completed in a timely manner.

Access cards and/or keys must be appropriately protected, not shared or transferred and returned when no longer needed. Lost or stolen cards/keys must be reported immediately.

The Company should ensure that visitors obtain security clearance before entering the premises. This could include, but is not limited to, a sign in book, employee escort within a secure area, ID check and ID badges for visitors.

Computers, printers and other non-portable information systems equipment belonging to the Company must not be removed from the Company's premises unless accompanied by an approved property pass issued by the IT Manager.

Equipment and media taken off premises should not be left unattended in public areas. Portable computers and personal digital assistants (PDA's) should be carried as hand luggage where possible when travelling.

#### 4. **POLICY NOTIFICATION**

The Head of the Company is responsible for ensuring that employees are aware of where policies are located on websites. The head of the Company is also responsible for notifying employees of policy change or the creation of new policies that pertain to the agency/department function.

## Anti-Virus Policy

Policy	Anti-Virus Policy
Document No.	POL APF

### 1. **PURPOSE**

The purpose of this policy is to establish requirements which must be met by all computers connected to the Company's networks and to ensure effective virus detection and prevention.

### 2. **SCOPE**

This policy applies to all of the Company's computers that are PC-based or utilize PC-file directory sharing. This includes, but is not limited to, desktop computers, laptop computers, file/ftp/tftp/proxy servers.

### 3. **POLICY**

- 3.1 All of the Company's PC-based computers must have the Company's standard, supported anti-virus software installed and scheduled to run at regular intervals. In addition, the anti-virus software and the virus pattern files must be kept up-to-date. Virus-infected computers must be removed from the network until they are verified as virus-free. The IT department is responsible for creating procedures that ensure anti-virus software is run at regular intervals, and computers are verified as virus-free. Any activities with the intention to create and/or distribute malicious programs into the Company's networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited, in accordance with the *Acceptable Use Policy*.
- 3.2 Users must not attempt to remove viruses themselves. If a virus infection is detected, users must disconnect from the Company's networks, stop using the infected computer immediately and notify the IT department.
- 3.3 Users must be cautious of e-mail attachments from an unknown source as viruses are often hidden in attachments. If a virus is suspected the attachment must not be opened or forwarded and must be deleted immediately.

### 4. **ENFORCEMENT**

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

## Surveillance and Monitoring Policy

Policy	Surveillance and Monitoring Policy
Document No.	POL APG

### 1. **PURPOSE**

The purpose of this policy is to prevent crime and assist the Company in protecting:

- The safety and property of the Company, its employees and visitors.
- The applicable legal and privacy interests of the Company, its clients and employees.

### 2. **SCOPE**

This policy applies to Company's, all permanent and temporary employees, contractors, consultants, including all personnel affiliated with third parties who use surveillance cameras in the Company and/or conduct surveillance monitoring and recording.

This policy does not apply to:

- The use of surveillance cameras or other surveillance conducts during criminal investigations, by the Company or by law enforcement agencies.

### 3. **DEFINITIONS**

#### 3.1 Surveillance Camera

Any item, system, camera, technology device, communications device used alone or in conjunction with a network for the purpose of gathering, monitoring, recording or storing an image or images of the Company and/or people at the premises of the Company. Images captured by surveillance cameras may be real-time or preserved for review at a later date. Such devices may include, but are not limited to the following:

1. Close-circuit television
2. Web cameras
3. Real-time surveillance systems
4. Computerized visual monitoring
5. Cell phone with cameras



### 3.2 Surveillance Monitoring or Recording

Using surveillance cameras or other related technology to observe, review or store visual images for the purpose of deterring crime and protecting the safety and security of the Company.

### 3.3 The Company premises

All areas on property owned, leased or controlled by the Company, both internal and external, including offices, common spaces, and other areas.

## 4. **POLICY**

The Company is committed to integrating the best security. The Company's use of surveillance cameras for surveillance monitoring or recording must be:

- Conducted in a professional, ethical, and legal manner.
- Compliant with the Company's Policies and Procedures.
- Limited to uses that does not violate a person's reasonable expectation of privacy, as defined by current legal requirements.

## 5. **PROCEDURES**

5.1 Installation and/or placement of surveillance cameras in the Company premises must be approved by the Director(s) and Information Officer of the Company.

5.2 Only employees designated by the Director(s) and/or Information Officer will have access to the images captured by surveillance monitoring or recordings.

5.3 All existing uses of surveillance cameras and surveillance monitoring or recording, subject to this policy, must be in compliance with this policy. A request to continue using the existing surveillance cameras will be submitted to the Information Officer. Network connectivity for surveillance monitoring or recording must comply with the Company's policies.

5.4 Violations of these procedures may result in disciplinary action in accordance with the policies, contracts, rules and regulations of the Company.

## 6. **TRAINING**

The Information Officer will ensure that the designated employees will be trained on the responsible use of the information and technology. Designated employees will also be supervised by a specific supervisor, with periodic review performed by the Information Officer or his/her deputy.

7. **RETENTION AND RELEASE OF INFORMATION**

- 7.1 The Company will retain images obtained through surveillance monitoring or recording for a length of time deemed appropriate for the purpose of monitoring, but not to exceed 90 days, unless such images have historical value, or are being used for a criminal investigation. Any questions regarding the retention of these images should be directed to the Information Officer.
- 7.2 Only the Director(s) and / or Information Officer can authorize the release of information and results obtained through surveillance monitoring or recording.
- 7.3 The IT department will ensure that all networks are backed up regularly in order to ensure the safeguarding of personal information.
- 7.4 Information obtained in violation of this policy cannot be used in any disciplinary proceeding against any employee.

## Data Retention Policy

Policy	Data Retention Policy
Document No.	POL APH

### 1. **PURPOSE**

The purpose of this policy is to ensure that necessary records and documents of the Company are adequately protected and maintained to ensure that records that are no longer needed by the Company or are of no value, are discarded at the proper time. This policy is also for the purpose of aiding employees of the Company in understanding their obligations in retaining documents.

### 2. **SCOPE**

This policy applies to all documents which are collected, processed or stored by the Company and includes but is not limited to documents in paper and electronic format, for example, e-mail, web and text files, PDF documents etc.

### 3. **ENFORCEMENT**

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

### 4. **GUIDELINES FOR THE RETENTION OF DOCUMENTS**

- 4.1 The Company may suspend the destruction of any record or document due to pending or reasonably foreseeable litigation, audits, government investigations or similar proceedings. Employees will be notified of applicable documents where the destruction has been suspended to which they have access to.
- 4.2 All documentation and personal information that is being stored by the Company in accordance with this policy must be stored and guarded in compliance with all the Company's policies.
- 4.3 The documentation and information listed below may not contain all the records and documents processed and in the possession of the Company and should merely be used as a guideline.
- 4.4 In the event that a document and/or information is no longer required to be stored in accordance with this policy and relevant legislation, it should be deleted and destroyed in accordance with the Data Destruction Policy of the Company.
- 4.5 The Information Officer should be consulted where there is uncertainty regarding the retention and destruction of a document and/or information.

## Accounting

<u>Nr</u>	<u>Type of document</u>	<u>Minimum Retention Required</u>
1	Annual Financial Statements including, annual accounts, director's and auditors report	15 Years
2	Books of accounting recording information required by the Companies Act No.71 of 2008	15 Years
3	Branch Register	5 Years
4	Certificate of change of name	Indefinite
5	Certificate of incorporation	Indefinite
6	Certificate to commence Company	Indefinite
7	Director's attendance register	15 Years
8	Index of members	15 Years
9	Memorandum and articles of association	Indefinite
10	Minute book, CM25 and CM26, as well as resolutions passed at the general/class meetings	Indefinite
11	Microfilm image of any original record reproduced directly by the camera	Indefinite
12	Proxy forms	3 Years
13	Proxy forms used at court convened meetings	3 Years
14	Register of allotments – after a person ceased to be a member	15 Years
15	Register of directors and certain officers	15 Years
16	Register of director's shareholding	15 Years
17	Register of Members	15 Years
18	Register of mortgages and debentures and fixed assets	15 Years

## Personnel Records

<u>Nr</u>	<u>Type of document</u>	<u>Minimum Retention Required</u>
1	Employee's employment contract	3 Years
2	Time worked by employee	3 Years
3	Remuneration to be paid to each employee	3 Years
4	Date of birth of any employee under 18 years of age	3 Years
5	Employee deduction authorisation	3 Years
6	Garnishments	3 Years
7	Employee disciplinary record	3 Years
8	Employee count records	3 Years

## Health and Safety

<u>Nr</u>	<u>Type of document</u>	<u>Minimum Retention Required</u>
1	Register, records or reproduction of the earnings, time worked, payment for piece work and overtime and other prescribed particulars of all the employees compensated for disablement caused by occupational injuries or diseases sustained or contracted by employees in the course of their employment, or for death sustained by these injuries at their place of work.	4 Years
2	A health and safety committee shall keep record of each recommendation made to an employer in terms of issues affecting the health of employees and of any report made to an inspector in terms of the recommendation.	3 Years
3	Records of incidents reported at work.	3 Years
4	Records of assessment and air monitoring, and the asbestos inventory.	Minimum of 40 years
5	Medical surveillance records	40 Years
6	Records of risk assessment and air monitoring results	40 Years
7	Medical surveillance records	40 Years
8	Records of assessment and air monitoring	30 Years
9	All records of assessments and noise monitoring	40 Years

## Credit Agreements

<b>Nr</b>	<b>Type of document</b>	<b>Minimum Retention Required</b>
1	Enquiries	2 Years
2	Payment profile	5 Years
3	Adverse information	1 Year
4	Civil court judgements	The earlier of 5 years or until the judgement is rescinded by a court or abandoned
5	Administration orders	The earlier of 10 years or until the order is rescinded by a court
6	Sequestrations	The earlier of 10 years or the order is rescinded by a court
7	Liquidations	Unlimited
8	Rehabilitation orders	5 Years

## Electronic Communication

<u>Nr</u>	<u>Type of document</u>	<u>Minimum Retention Required</u>
1	Personal information and the purpose for which the data was collected must be kept by the person who electronically requests, collects, collates processes or stores the information	As long as the information is used and at least 1 year thereafter
2	A Record of any third party to whom the information was disclosed	As long as information is used and at least 1 year thereafter
3	All personal data that has become obsolete	Destroy

## Miscellaneous

<u>Nr</u>	<u>Type of document</u>	<u>Minimum Retention Required</u>
1	Employment record – all non-hired applicants (including all applications and resumes – whether solicited or unsolicited, results of post-offer, pre-employment physicals, results of background investigations, if any, related correspondence.	3 Years
2	Client Files	5 Years

## Data Destruction Policy

Policy	Data Destruction Policy
Document No.	POL API

### 1. **PURPOSE**

The purpose of this policy is to provide guidance to the Company's employees regarding the destruction of documentation. All forms of computer equipment, digital storage media and printed or handwritten material must be disposed of securely when no longer required. Secure disposal maintains our data security and supports compliance with the Company policies and procedures.

The Company realises that electronic devices and media can hold vast amounts of information, some of which can linger indefinitely and sees compliance of this policy as of the utmost importance in order to ensure that restricted data and/or personal information does not find its way into unauthorised hands.

### 2. **SCOPE**

This Policy aims to protect restricted data and personal information and applies to all users of the Company's network including Director(s), Manager(s), administrative personal, other employees, contractors, visitors and third parties. The Policy applies to all information systems owned by the Company and includes personal computers, Macs, laptops, mobile phones, handheld computers, servers and external or removable storage devices. The Policy also applies to printed materials.

### 3. **SECURE DISPOSAL**

- 3.1 In determining whether a document and/or information should be stored or disposed of, each employee should first refer to the Data Retention Policy and in the event of any uncertainties, to the Information Officer of the Company.
- 3.2 Under no circumstances should paper documents or removable media (CD's, DVD's, discs, etc.) containing personal or confidential information be simply binned or deposited in refuse tips.
- 3.3 The Company will ensure that all electrical waste, electronic equipment and data on disk drives be physically removed and destructed in such a way that the data will by no means be able to be virtually retrieved.
- 3.4 Employees must ensure that all paper documents that should be disposed of, be shredded locally within the department and then be recycled.

Where local shredding is not possible, bulk quantities of restricted paper waste must be held in waste sacks. These will be collected and disposed of by an employee instructed to do so by the Information Officer.

- 3.5 In the event that a third party is used for data destruction purposes, this third party must also comply with the regulations as stipulated in this policy and any other applicable legislation.



## Risk Management Policy

Policy	Risk Management Policy
Document No.	POL APJ

### 1. **PURPOSE AND SCOPE**

This policy establishes the process for the management of risks faced by the Company. The aim of risk management is to maximise opportunities in all the Company activities and to minimise adversity. The policy applies to all activities and processes associated with the normal operation of the Company. It is the responsibility of all Director(s), permanent and temporary employees to identify, analyse, evaluate, respond, monitor and communicate risks associated with any activity, function or process within their relevant scope of responsibility and authority.

### 2. **DEFINITIONS**

2.1 “Risk”: is the likelihood that a harmful consequence (death, injury or illness) might result when exposed to a hazard. Risk is characterised and rated by considering two characteristics:

- Probability or likelihood of occurrence; and
- Consequence (C) of occurrence.

This is expressed as  $R \text{ (risk)} = L \text{ (likelihood)} \times C \text{ (consequence)}$ .

2.2 “Likelihood”: is a qualitative description of probability or frequency.

2.3 “Consequence”: is the outcome of an event, being a loss, injury, disadvantage or gain. There may be a range of possible outcomes associated with an event.

2.4 “Risk control”: means taking action to first eliminate risk so far as is reasonably practicable, and if that is not possible, minimising the risks so far as is reasonably practicable. Eliminating a hazard will also eliminate any risks associated with that hazard. Risk Assessment is the process of evaluating and comparing the level of risk against predetermined acceptable levels of risk.

2.5 “Risk Management”: is the application of a management system to risk and includes identification, analysis, treatment and monitoring.

2.6 “Risk Owner”: is the person(s) responsible for managing risks and is usually the person directly responsible for the strategy, activity or function that relates to the risk.

### 3. **PRINCIPLES**

The Company is proactive in its approach to risk management, balances the cost of managing risk with anticipated benefits, and undertakes contingency planning in the event that critical risks are realised.

The Company has the primary duty to ensure the health and safety of workers and other persons at the workplace, which includes the realisation of all other rights in this or any other act.

### 4. **FUNCTIONS AND DELEGATIONS**

The Information Officer should exercise due diligence to ensure that the Company complies with the Protection of Personal Information Act and this Policy. This includes taking reasonable steps to:

- gain an understanding of the hazards and risks associated with the operations of the Company; and
- ensure that the Company has and uses appropriate resources and processes to eliminate or minimise risks to health and safety.

All Board members and employees must contribute to the establishment and implementation of risk management systems for all functions and activities of the Company. These risk management Company's must align with all policies and applicable legislation.

### 5. **POLICY DETAIL**

The Company aims to achieve better Company in the management of risks that threaten to adversely impact on the Company its functions, objectives, operations, assets, staff, consumers or members of the public. The Company does whatever it can (whatever is 'reasonably practicable') to ensure its workers, consumers and other people are not harmed by its activities.

### 6. **RISK MANAGEMENT PRINCIPLES**

The Company has to take into consideration the following aspects in adhering to risk management compliance:

- Consulting with employees:  
It is imperative that the employees of the Company are made aware of the inherent risks that they are exposed to concerning their health and safety. It is important to have regular meetings with such employees in order to make sure that the employees have a thorough understanding of the processes and procedures in place to minimize such risk.

- Identify hazards:

Care should be taken in identifying the hazards associated with the day to day operations of the Company. These hazards include, but is not limited to the physical work environment, the equipment, materials and substances used, the work tasks and how they are performed. It is important to note the employees should be aware of these hazards as well as the precautions that need to be taken in order to minimize the potential damage.

- How to assess risks:

Your Consumer Protection legal advisor will assist in identifying the potential risk areas of the Company. He/she will also advise you on the appropriate measures to be implemented in order to minimize these risks.

- How to control risks:

It is important that upon identifying potential risk areas that appropriate measures be put in place in order to control and/or minimize those risk areas. Where it is possible for the hazard or risk to be eliminated completely, this should be done without delay. The responsible person who oversees this potential risk area must be made aware of such risk in order to implement appropriate safeguards.

- How to review controls:

It is important that the Company reviews the control measures in place to eliminate and minimize the risk areas on a regular basis.

- How to keep records:

It is essential that the Company documents and stores all applicable information regarding potential risk areas, as well as the decisions that was made and implemented in order to address those risk areas. These documents should be stored in accordance with the Data Retention Policy, as well as applicable legislation.

## 7. **ROLE AND RESPONSIBILITY OF THE I/O**

The Company has to take into consideration that the elected Information Officer needs to ensure that all employees, subcontractors, representatives, agents and suppliers have a reasonable understanding of the hazards and risks associated with the day to day responsibilities and operations in ensuring that the Company uses all appropriate resources and available processes to eliminate the Company's risk element.

## Information Classification Policy

Policy	Information Classification Policy
Document No.	POL APK

### 1. **PURPOSE**

It is critical for the Company to set the standard for the protection of information assets from unauthorized access and compromise or disclosure. Accordingly, the Company has adopted this information classification policy to help manage and protect its information assets.

### 2. **RESPONSIBILITY**

All of the Company's employees share in the responsibility for ensuring that the Company information assets receive an appropriate level of protection by observing this Information Classification policy:

- Managers of the Company or information "Owners" shall be responsible for assigning classifications to information assets according to the standard information classification system presented below: "Owners" have approved management responsibility, "Owners" do not have property rights.)
- Where practicable, the information category shall be embedded in the information itself.
- All employees of the Company shall be guided by the information category in their security-related handling of the Company's information.

All information of the Company and all information entrusted to the Company from third parties fall into one of three classifications in the table below, presented in order of increasing sensitivity.

<u>Information Description</u>	<u>Category:</u>	<u>Examples:</u>
Unclassified Public	Information is not confidential and can be made public without any implications for the Company.	<ul style="list-style-type: none"> <li>• Product brochures widely distributed</li> <li>• Information widely available in the public domain, including publicly available web site areas of the Company</li> </ul>

		<ul style="list-style-type: none"> <li>• Sample downloads of the Company's software that is for Sale</li> <li>• Financial reports required by regulatory authorities</li> <li>• Newsletters for external transmission</li> </ul>
Proprietary	Information is restricted to management approved internal access and protected from external access. Unauthorized access could influence the Company's operational effectiveness, cause an important financial loss, provide a significant gain to a competitor, or cause a major drop in customer confidence. Information integrity is vital.	<ul style="list-style-type: none"> <li>• Passwords and information on corporate security procedures</li> <li>• Know-how used to process client information</li> <li>• Standard Operating Procedures used in all parts of the Company activities</li> <li>• All software codes developed by the Company, whether used internally or sold to clients</li> </ul>
Client / Client Confidential Data	Information collected and used by the Company in the conduct of its Company to employ people, to log and fulfil client orders, and to manage all aspects of corporate finance. Access to this information is very restricted within the Company. The highest possible levels of integrity, confidentiality, and restricted availability are vital.	<ul style="list-style-type: none"> <li>• Salaries and other personnel data</li> <li>• Accounting data and internal financial reports</li> <li>• Confidential customer Company data and confidential contracts</li> <li>• Non-disclosure agreements with clients\vendors Company plans</li> </ul>

## Clean Desk and Clear Screen Policy

Policy	Clean Desk and Clear Screen Policy
Document No.	POL APL

### 1. **INTRODUCTION**

#### 1.2 In the event that

- (i) personal information, as this is defined in the Protection of Personal Information Act 4 of 2013 ("POPIA"), and / or
- (ii) other confidential, sensitive or restricted information, is not securely stored away when not directly in use, the Company could be at risk of suffering a data breach, which can cause it reputational and other damage.

#### 1.2 All (i) employees, (ii) contractors, (iii) visitors, and / or (iv) other persons authorised to access and use the Company's systems, "Users" are required to keep their

- (i) their Desks and Tables, and (ii) Screens clear of all personal information in terms of POPIA (Personal Information) and / or confidential, sensitive and / or proprietary information belonging to the Company (Confidential Information) when such information is not being used or accessed by the User in question.

### 2. **PURPOSE**

#### 2.1 The purpose of this policy is to ensure that all paper and electronic records containing Personal Information and / or any other Confidential Information are suitably secured when not in use and are not left visible on an unattended

- (i) Desk and Table, or
- (ii) Screen.

#### 2.2 This Policy applies to all working areas, including Desks and Tables, which must not have any Personal Information and / or Confidential Information displayed on them whilst unattended for any period of time. In the event that the User in question is working on any Company system or device remotely, such User must also ensure that the provisions of this Policy are strictly adhered to at all times.

#### 2.3 Controlling physical access to the information assets within the Company is vitally important. This relies upon physical, technological and policy Controls to ensure that the Company operates within a secure environment at all times, protecting personnel, facilities, information and data from the risk of:

##### 2.3.1 loss or damage of information resources;

- 2.3.2 unauthorised access to information resources;
- 2.3.3 disruption and / or destruction of information processing facilities; and
- 2.3.4 breach of relevant legislation, including POPIA, and / or non-compliance with regulatory standards.

### 3. **SCOPE**

This Policy applies to all Users, and any and all functions and departments within the Company where Personal Information and / or Confidential Information are created, accessed, updated, stored, maintained, managed or even deleted.

### 4. **RELATED DOCUMENTS**

This Policy is to be read together with the Company's Acceptable Usage Policy, which also deals with the Company's information security policies and procedures.

### 5. **DEFINITIONS**

- 5.1. In this Policy, in addition to the other terms that have been defined in the body of the Policy, the Company makes use of the following terms:

5.1.1. "Controls" means control measures put in place by the Company to mitigate the risks identified to the security of Personal Information and / or Confidential Information, including instituting and implementing policies and procedures, management control, reporting, physical security measures and the like;

5.1.2. "Desk/s and Table/s" means any physical working area where Personal Information and / or Confidential Information is processed, including printing areas, whether situated at the Company's premises or remotely; and

5.1.3. "Screen/s" means any monitor on any device upon which Personal Information and / or Confidential Information is stored that displays such information.

- 5.2. In addition, unless the contrary is specified, terms that are used in the Policy that are specifically defined in POPIA, are given the meanings ascribed to them in POPIA.

### 6. **POLICY**

- 6.1. All Users are required, and undertake, to apply a (i) clean Desk and Table, and (ii) clear Screen policy, as this will help to protect the Company's information assets from being compromised in any way. Without detracting from the generality of the foregoing obligations on Users in terms of this Policy, the following actions must be taken to ensure that the necessary Controls are in place:

- 6.1.1. Users must ensure that all Personal Information and / or Confidential Information stored in both hardcopy or electronic form is secured in their Desk and Table at the end of each day and when they are expected to be away from their Desk and Table;
- 6.1.2. Screens must be locked when a User's Desk and Table is unoccupied;
- 6.1.3. All Personal Information and / or Confidential Information, in whatever format this may be stored, must be locked in a drawer or cupboard at the end of each day and when the desk is unoccupied;
- 6.1.4. Filing cabinets containing Personal Information and / or Confidential Information must be kept closed and locked at the end of each day and when not in use or when unattended;
- 6.1.5. Keys used to access and Personal Information and / or Confidential Information must not be left at or on an unattended Desk and Table;
- 6.1.6. Laptops and computers must be either locked with a secure locking mechanism or locked away in a drawer or cabinet at the end of each work day or when they are left unattended;
- 6.1.7. Passwords may not be left on any sticky or other notes posted on or under a computer or laptop, nor may they be left written down in an accessible location;
- 6.1.8. Printouts containing any Personal Information and / or Confidential Information must be removed from the printer immediately;
- 6.1.9. All Personal Information and / or Confidential Information that is ready to be disposed of must be placed in the designated confidential disposal bins to be shredded or otherwise securely destroyed;
- 6.1.10. Whiteboards containing Personal Information and / or Confidential Information should be erased as soon as reasonably possible; and
- 6.1.11. All mass storage devices, including CDRoms, DVDs or USB drives must be treated as sensitive and must be secured in a locked drawer.

## **7. RIGHTS RESERVED BY THE COMPANY**

The Company reserves the right to monitor, audit, screen, and preserve Company information as the Company deems necessary, in its sole discretion, in order to maintain compliance with this Policy and, by extension, all relevant provisions of POPIA. Any dissemination, unauthorised use or benefit from any Company information by a User in contravention of this Policy may result in disciplinary action being taken against such User by the Company. Furthermore, the use of any account or system in such a way that breaches any of the provisions of this Policy will be reported to the appropriate supervisor or manager within the Company, which may lead to further disciplinary action being taken.



## 8. **ENFORCEMENT AND POTENTIAL DISCIPLINARY ACTIONS**

Any violation of this Policy may result in disciplinary action being taken against the User in question. Such disciplinary action will be taken in accordance with the Company's applicable disciplinary code, and may include the

- (i) termination of employment in relation to employees of the Company,  
**or**
- (ii) cancellation or termination of contractual relations in the case of other Users, such as contractors or consultants. Notwithstanding the foregoing, should any authorised User fail to adhere to this policy, the individual will be dealt with as prescribed by the Company's disciplinary code and procedures.

## 9. **POLICY AWARENESS AND UPDATES**

- 9.1. Training and awareness: The (i) requirement for, and (ii) a User's obligation in terms of, this Policy will be explained in detail in the Company's induction program, in the case of employees of the Company. Further training and additional awareness regarding the Policy will be offered from time to time by the Company. The Company will specifically make Users who are not employees of the Company aware of the Policy.
- 9.2. Dissemination: This Policy will be made available on the Company's network, intranet or similar portals.
- 9.3. Review: This Policy will be reviewed from time to time in order to ensure ongoing compliance with POPIA, but such revisions will take place at least annually. More frequent review may be required in response to
  - (i) exceptional circumstances,
  - (ii) organisational change, or
  - (iii) relevant changes in legislation or guidance.

## Backup and Restoration Policy and Procedure

Policy	Backup and Restoration Policy and Procedure
Document No.	POL APM

### 1. **INTRODUCTION**

- 1.1. The Company is responsible for ensuring the confidentiality, integrity, and availability of the data and information stored on its systems.
- 1.2. The Backup and Restoration of data is an important aspect to ensure the availability of information / data for the Company.

### 2. **OBJECTIVE**

The objective of this policy and procedure ("Policy") is to formalise the Backup and Restoration process adopted by the Company. The process of Backing up data is pivotal to a successful disaster recovery plan ("DRP").

### 2. **SCOPE**

- 2.1. This Policy applies to (i) employees, (ii) contractors, (iii) visitors, and / or (iv) other persons authorised to access and use the Company's systems ("Users").
- 2.2. This Policy covers all servers, workstations, network devices, operating systems, applications and other information assets belonging to the Company.

### 3. **TERMS AND ABBREVIATIONS**

- 3.1. In this Policy, in addition to the other terms that have been defined in the body of the Policy, the Company makes use of the following terms:
  - 3.1.1. "Backup" means the copying of physical or virtual files or databases to a secondary location for preservation to assist in the event of equipment failure or catastrophe;
  - 3.1.2. "Restoration" means the process of restoring something to its former condition and, in the case of a computer or other electronic device, means returning it to a previous state, including
    - (i) restoring a previous system backup or the original factory setting, or
    - (ii) restoring data that was on the system;
  - 3.1.3. "CIO" means the chief information officer of the Company; and

3.1.4. "IT User" means a User within the Company authorised to be responsible for the carrying out of the Company's necessary information technology ("IT") functions.

3.2. In addition, unless the contrary is specified, terms that are used in the Policy that are specifically defined in POPIA, are given the meanings ascribed to them in POPIA.

#### 4. **DOCUMENTS**

This Policy should be read in conjunction with the Company's Acceptable Usage Policy insofar as it relates to IT aspects.

#### 5. **POLICY**

5.1. The extent, frequency and retention period of Backups must reflect:

5.1.1. the Company's Company requirements;

5.1.2. the Company's security requirements of the information involved;

5.1.3. how critical the information is to the Company's continued Company operations;

5.1.4. the retention period for essential Company information; and

5.1.5. any requirement for archived copies to be permanently retained by the Company.

5.2. The extent, frequency and retention periods of the Backups must be reviewed regularly and, in each case, where circumstances change or failures occur.

5.3. Backup arrangements must meet the requirements of the Company's Company continuity plans.

5.4. The Company's critical systems must be clearly identified, and, for such systems, the Backup arrangements must cover all system information, applications, and data necessary to recover the complete system in the event of a disaster.

5.5. Where Backup arrangements are automated, such automated solutions must be sufficiently tested prior to implementation and at regular intervals thereafter.

5.6. All Backup media must be appropriately labelled with dates and codes / markings which enables easy identification of the original source of the data and the type of Backup used on the media.

5.7. Where the confidentiality of the information is important, Backups must be protected by encryption and all encryption keys must be kept securely at all times, with clear procedures in place to ensure that Backup media can be promptly decrypted as required.

- 5.8. Accurate and complete records of the Backup copies must be retained both locally and remotely and afforded the same level of physical and environmental protection as other important documentation. Such records should include information pertaining to the department in question, data location, date of Backup, type of Backup and the like.
- 5.9. Copies of Backup media must be removed from all Company devices as soon as reasonably possible when a Backup or Restoration has been completed.
- 5.10. Backup media which is retained on-site at the Company, prior to being sent for storage at a remote location, must be stored securely at a sufficient distance away from the original data source to ensure that both the original and Backup copies are not compromised.
- 5.11. Access to the retained Backup media must be restricted to authorised staff only.
- 5.12. All Backups identified for long term storage must be stored at a secure remote location with appropriate environmental control and protection to ensure continuing media integrity.
- 5.13. Backup media must be protected in accordance with the Company's physical, environmental, data protection and media handling policies and procedures.
- 5.14. Restoration processes must be checked and tested regularly to ensure that they are effective and that they can be completed within the time allotted in the operational procedures for recovery.
- 5.15. Hard copy paper files containing important information and data must also be digitised and stored in a location where they will be Backed up by the Company in the same manner as electronic information.
- 5.16. Where Backups fail, data and system owners must be promptly informed and a record maintained. Such a record must include information regarding any action taken by the Company to address such failure.
- 5.17. Backup data / media no longer required must be clearly marked and recorded for secure disposal or destruction, with due environmental consideration.
- 5.18. Where provision is made in this Policy for reviews to be done at regular intervals, such intervals will be determined by the CIO in his / her sole discretion.

## 6. **PROCEDURE**

- 6.1. There are 5 (Five) common types of backup, they are:
  - 6.1.1. Full Backup: A full Backup is when every single file and folder in the Company's systems is Backed up. A full Backup takes longer and requires more space than other types of Backups. However, the process of Restoring lost data from the Backup is much faster.

- 6.1.2. Incremental Backup: With incremental Backups only the first Backup is a full Backup. Subsequent Backups only store changes that were made after the previous Backup. The process of Restoring lost data from the Backup is longer, however, the Backup process itself is much quicker.
- 6.1.3. Differential Backup: A differential Backup is similar to an incremental Backup. With both, the first Backup is full and subsequent Backups only store changes made to files after the last Backup. This type of Backup requires more storage space than an incremental Backup does, however, it also allows for a faster Restoration time.
- 6.1.4. Mirror Backup: A mirror Backup is when an exact copy is made of the source data. The advantage of mirror Backups as opposed to full, incremental, or differential Backups, is that old, obsolete files are not being stored. When obsolete files are deleted, they are also deleted from the mirror Backup when the system Backs up. The disadvantage of a mirror Backup is that, if files are accidentally deleted, they may also be lost from the Backup if the deletion is not discovered prior to the next scheduled Backup.
- 6.1.5. Replication Backup: A replication Backup occurs where data stored on servers is replicated between different servers. Sometimes these servers may be in the same data centre. If the Backup is a pure replication, there is a risk that if the data on the main server is corrupted, the rest of the replicated data could also be corrupted. When implementing replication Backups, a Backup that is at least 1 (One) day older than the live data must be kept to manage this risk.
- 6.2. Backup schedule: Item 2 of the Schedule sets out the Backup schedule of the Company, which must be reviewed and updated on a regular basis. Item 2 includes the following information:
  - 6.2.1. The system / device to be Backed up;
  - 6.2.2. The location of such device;
  - 6.2.3. The type of Backup that was implemented, including:
    - full Backup;
    - incremental Backup;
    - differential Backup;
    - mirror Backup; and / or
    - replication Backup;
  - 6.2.4. The frequency of the Backup; and
  - 6.2.5. The person responsible for the Backup.

- 6.3. Retention period of Backups: Item 3 of the Schedule sets out the retention periods of Backups implemented within the Company. This schedule must be reviewed and updated on a regular basis. Item 3 includes the following information:
- 6.3.1. The system/device Backed up;
  - 6.3.2. The location of such device;
  - 6.3.3. The type of Backup that was implemented, including:
    - full Backup;
    - incremental Backup;
    - differential Backup;
    - mirror Backup; and / or
    - replication Backup; and
  - 6.3.4. The retention period of the Backup in question.
- 6.4. IT Users responsibilities
- 6.4.1. IT Users must ensure that data is securely maintained and is available for Backup at all times.
  - 6.4.2. IT Users must store any data / files that require Backup on their allocated network storage area and not on local hard drives.
  - 6.4.3. If the allocated storage area becomes unavailable, IT Users may not temporarily save the data locally on hard drives or on a USB data stick, but must promptly contact the CIO to Restore the data in question.
- 6.5. Data Restoration
- 6.5.1. Data (file) Restoration must only be done by competent, authorised staff within the Company.
  - 6.5.2. The following procedure must be followed when performing Restorations:
    - IT Users must request the Restoration of data by contacting the CIO;
    - The CIO must verify that the IT User has permission or authorisation to view or Restore data prior to any Restoration taking place;
    - The CIO must request the following information from the IT User in order to facilitate the Restoration:
      - The reason for the Restoration;
      - The names of files or folders to be Restored;
      - The original location of the files or folders to be Restored;

- The IT User's best estimation of the date and time when the IT User noticed the deletion / corruption in question; and
- The IT User's best estimation of the date and time when the IT User recalls the files or folders in question being accessible and intact;
- Requests from third party software / hardware vendors for file or system Restorations for the purpose of system support, maintenance, testing or other unforeseen circumstance must be made to the CIO;
- IT Users accessing Backup media for the purpose of a Restoration must ensure that any media used is returned to a secure location when it is no longer required; and
- A log must be maintained to record the use of Backup media whenever it has been requested and / or removed from secure storage.

## **7. RIGHTS RESERVED BY THE COMPANY**

The Company reserves the right to monitor, audit, screen, and preserve Company information as the Company deems necessary, in its sole discretion, in order to maintain compliance with this Policy and, by extension, all relevant provisions of the Promotion of Access to Information Act 4 of 2013 ("POPIA"). Any dissemination, unauthorised use or benefit from any Company information by a User in contravention of this Policy may result in disciplinary action being taken against such User by the Company.

Furthermore, the use of any account or system in such a way that breaches any of the provisions of this Policy will be reported to the appropriate supervisor or manager within the Company, which may lead to further disciplinary action being taken.

## **8. ENFORCEMENT AND POTENTIAL DISCIPLINARY ACTIONS**

Any violation of this Policy may result in disciplinary action being taken against the User in question. Such disciplinary action will be taken in accordance with the Company's applicable disciplinary code, and may include the

- (i) termination of employment in relation to employees of the Company, or
- (ii) cancellation or termination of contractual relations in the case of other Users, such as contractors or consultants. Notwithstanding the foregoing, should any authorised User fail to adhere to this policy, the individual will be dealt with as prescribed by the Company's disciplinary code and procedures.

## **9. POLICY AWARENESS AND UPDATE**

### **9.1. Training and awareness: The**

- (i) requirement for, and
- (ii) a User's obligation in terms of, this Policy will be explained in detail in the Company's induction program, in the case of employees of the Company. Further training and additional awareness regarding the Policy will be offered from time to time by the Company. The Company will specifically make Users who are not employees of the Company aware of the Policy.

### **9.2. Dissemination: This Policy will be made available on the Company's network, intranet or similar portals.**

### **9.3. Review: This Policy will be reviewed from time to time in order to ensure ongoing compliance with POPIA, but such revisions will take place at least annually. More frequent review may be required in response to**

- (i) exceptional circumstances,
- (ii) organisational change, or
- (iii) relevant changes in legislation or guidance.



## Bring Your Own Device (BYOD) Policy

Policy	Bring Your Own Device (BYOD) Policy
Document No.	POL APN

### 1. **INTRODUCTION**

- 1.1. Bring your own Device ("BYOD") is the Company of allowing employees and other authorised persons that perform work for the Company to use their own personal devices for work purposes. This includes, without limitation, mobile phones, laptops and tablets. The use of such personal devices for Company purposes will be referred to as BYOD, or the BYOD initiative, for purposes of this Policy.
- 1.2. It is imperative for the Company to protect and secure the data or information that it processes, both for reputational reasons and to ensure compliance with the provisions of the
  - (i) Protection of Personal Information Act no. 4 of 2013 ("POPIA"), applicable to the processing of personal information, as this term is defined in POPIA ("Personal Information"), in South Africa, and / or
  - (ii) General Data Protection Regulation of the European union, that will apply where the personal information of European citizens is processed by the Company.

### 2. **PURPOSE**

The purpose of this policy ("Policy") is to set out how the Company will retain control over its information while such information is being accessed through devices that are not owned by the Company.

### 3. **SCOPE**

This Policy applies to all (i) employees, (ii) contractors, (iii) visitors, and / or (iv) other persons authorised to access and use the Company's systems ("Users") that make use of personally-owned devices to process, store or transfer any information for purposes of conducting Company for the Company. This Policy applies to all Users irrespective of whether they make use of personal devices for Company at the premises of the Company ("Premises") or remotely.

Initial, the objective of this policy and procedure ("Policy") is to formalise the Backup and Restoration process adopted by the Company. The process of Backing up data is pivotal to a successful disaster recovery plan ("DRP").

#### **4. DOCUMENTS**

This policy should be read in conjunction with other Company policies that regulate the security of information including, without limitation, the Acceptable Usage Policy.

#### **5. POLICY**

- 5.1. The Company supports the use of BYOD for work purposes. The Company restricts the use of BYOD only to a limited number of Users who would not otherwise be in a position to perform the work, after proper authorisation, from the chief information officer of the Company ("CIO"), has been obtained.
- 5.2. All information belonging to the Company that is stored, transferred or processed on BYOD devices remains under the Company's ownership at all times, and the Company retains the right to regulate such information, and the processing of it, even though it is not the owner of the BYOD

#### **6. PROCEDURE**

##### **6.1. Permitted use of BYOD**

- 6.1.1. The CIO will create a list of Users with (i) job titles, in the event that Users are employees, or (ii) "relationship to Company", in the event that Users are not employees, who are authorised to use BYOD, together with the applications and / or databases they are allowed to access with their own personal device;
- 6.1.2. A User's request for access (using a mobile users access form) to participate in the BYOD initiative must be formally completed, and must be authorised by the CIO in writing before any access is granted to such User; and
- 6.1.3. Only Users that need information to perform their duties effectively with a BYOD device will be granted permission to use their own devices in terms of this Policy.

##### **6.2. Permitted devices**

- 6.2.1. The CIO will create and maintain a list of acceptable devices which can be used as BYOD, together with mandatory settings to be deployed for each device.

##### **6.3. Acceptable usage**

- 6.3.1. In addition to all of the provisions contained in the Acceptable Usage Policy, which also apply to this Policy, the following requirements are mandatory for every BYOD User:
  - Users must set and use a strong passcode to access personal devices;
  - Users must not share passcodes with anyone else;
  - Users must set devices to lock automatically when the device is inactive for more than 1 (One) minute;

- The latest and most secure antivirus software must be installed on each device and updated regularly;
- Patches and updates to operating systems of devices must be installed regularly;
- Each device must be configured to enable the device in question to be remotely-wiped should it be misplaced;
- Personal Information, and / or sensitive, critical, confidential and / or proprietary information of the Company (“Confidential Information”) must be protected by the most stringent security measures available (such as two pin authentication);
- When using BYOD off the Premises, Users must ensure that all devices are not left unattended and, if possible, these should be physically locked away;
- When using BYOD in public places, Users must ensure that no Company information can be read by unauthorised persons; and Initial
- Users must notify the CIO before any device used in the BYOD initiative is being disposed of, sold and / or handed to a third party for servicing.

#### 6.4. Prohibited uses of BYODs

##### 6.4.1. BYOD Users are prohibited from doing the following with devices used in the BYOD initiative:

- Allow anyone else access to the device in question;
- Install unknown and untrusted applications;
- Store illegal material on the device;
- Install unlicensed software;
- Connect via Bluetooth to any unknown devices;
- Connect to unknown wifi networks;
- Locally store passwords;
- Configure logins to save passwords for applications;
- Locally store any information that is (i) Personal Information, and / or (ii) Confidential Information; and
- Transfer any Company information to any unauthorised devices, including private / home devices.

#### 6.5. Special rights

##### 6.5.1. The Company has the right to view, edit, and delete all Company information that is stored, transferred or processed on a BYOD without the consent of the owner of the device in question.

#### 6.6. Reimbursement

##### 6.6.1. The Company will pay for the following:

- Software required by the Company in order to manage and control Company related information stored on any authorised device; and
- Other approved applications required to fulfil the duties or responsibilities of the relevant User.

#### 6.7. Security breaches

- 6.7.1. All security breaches related to the BYOD initiative must be reported immediately to the CIO.
- 6.7.2. All security or other related weaknesses that Users become aware of that have not yet become security incidents or breaches must be reported to the CIO by the User within 24 (Twenty-Four) hours of the User becoming aware of any such weakness.

### 7. **RIGHTS RESERVED BY THE COMPANY**

The Company reserves the right to monitor, audit, screen, and preserve Company information as the Company deems necessary, in its sole discretion, in order to maintain compliance with this Policy and, by extension, all relevant provisions of POPIA. Any dissemination, unauthorised use or benefit from any Company information by a User in contravention of this Policy may result in disciplinary action being taken against such User by the Company. Furthermore, the use of any account or system in such a way that breaches any of the provisions of this Policy will be reported to the appropriate supervisor or manager within the Company, which may lead to further disciplinary action being taken.

### 8. **ENFORCEMENT AND POTENTIAL DISCIPLINARY ACTIONS**

Any violation of this Policy may result in disciplinary action being taken against the User in question. Such disciplinary action will be taken in accordance with the Company's applicable disciplinary code, and may include the

- (i) termination of employment in relation to employees of the Company, or
- (ii) cancellation or termination of contractual relations in the case of other Users, such as contractors or consultants. Notwithstanding the foregoing, should any authorised User fail to adhere to this policy, the individual will be dealt with as prescribed by the Company's disciplinary code and procedures.

### 9. **POLICY AWARENESS AND UPDATE**

#### 9.1. Training and awareness: The

- (i) requirement for, and
- (ii) a User's obligation in terms of, this Policy will be explained in detail in the Company's induction program, in the case of employees of the

Company. Further training and additional awareness regarding the Policy will be offered from time to time by the Company. The Company will specifically make Users who are not employees of the Company aware of the Policy.

9.2. Dissemination: This Policy will be made available on the Company's network, intranet or similar portals.

8.3. Review: This Policy will be reviewed from time to time in order to ensure ongoing compliance with POPIA, but such revisions will take place at least annually. More frequent review may be required in response to

- (i) exceptional circumstances,
- (ii) organisational change, or
- (iii) relevant changes in legislation or guidance.

## Physical and Environmental Security Policy

Policy	Physical and Environmental Security Policy
Document No.	POL APO

### 1. **INTRODUCTION**

- 1.1. This policy ("Policy") sets out the requirements for protecting the information and technology resources and assets belonging to the from physical and environmental threats in order to reduce the risk of (i) loss, theft, damage and / or unauthorised access to those resources, or (ii) interference with, and disruption to, the Company's operations.

### 2. **PURPOSE**

The purpose of this Policy is to ensure that the Company implements measures focused on the physical and environmental control measures put in place to protect the Company's information and technology resources and assets.

### 3. **FURTHER PURPOSE**

- 3.1. This Policy applies to all departments and functions that use information and technology resources and assets to create, access, update, store, maintain and / or manage information or data to perform their Company functions. This information includes personal information as this term is defined in the Protection of Personal Information Act 4 of 2013 ("POPIA").
- 3.2. This Policy applies to all (i) employees, (ii) contractors, (iii) visitors, and / or (iv) other persons authorised to access and use the Company's systems ("Users").
- 3.3. Unless the contrary is specified, to the extent that any terms used in this Policy are defined in POPIA, such terms will be given the meaning ascribed to them in POPIA

### 4. **RELATED DOCUMENTS**

- 4.1. This Policy is read together with the other policies of the Company that regulate the use and protection of the Company's assets, including its information. In the event of any inconsistency between this Policy and other policies of the Company, the policy that provides the greatest protection to the Company and its assets will prevail.

### 5. **POLICY**

All Users and the Company's property, information and technology resources and assets should have appropriate physical and environmental security controls applied to mitigate the identified and potential information security risks to these assets. Such risks include (i) fire, natural disasters,

burglary, theft, vandalism, and terrorism (physical security risks), and (ii) electrical surges, flooding and natural disasters (environmental security risks).

## **6. KEY PRINCIPLES**

### **6.1. Risk assessment and treatment**

6.1.1. A security risk assessment of physical and environmental threats to Users, property, information and technology resources and assets of the Company must be conducted on an annual basis, unless required more frequently in terms of any other policy of the Company. Based on the outcome of the risk assessment conducted, appropriate key controls must be implemented by the Company to mitigate the risk.

### **6.2. Physical security**

6.2.1. Appropriate physical security measures must be identified in relation to the type of information or data that is required to be protected. For example, where there is an area within the Company's premises that visitors can access, but where no (i) Personal Information, and / or (ii) sensitive, confidential, proprietary and / or critical information of the Company ("Confidential Information") is kept, a lower level of physical security will be required than for an area where (i) Personal Information, and / or (ii) Confidential Information is stored or otherwise processed by the Company. A map of the Company's premises ("Premises") will be provided. This will then be colour-coded into areas that are either low, medium or high risk. Appropriate physical controls must then be implemented in relation to all areas within the Premises. The areas in the Premises should be classified as follows:

- Public areas such as the reception, the canteen, the boardrooms in the open areas may be classified as a low risk;
- Controlled areas such as general working areas or boardrooms within these working areas may be classified as a medium risk; and
- Highly restricted areas such as the information technology department, server room, finance department, human resources department and other areas where (i) Personal Information, and / or (ii) Confidential Information are processed may be classified as high risk.

6.2.2. Physical security measures must be implemented which will include:

- Security guards at the entrance where visitors enter the premises;
- An armed response that can be activated in the case of an emergency;
- Alarm systems that will be activated when the building is unoccupied to ensure intrusion detection;
- Cameras at strategic points to ensure that activities are monitored, recorded and stored;

- Physical Access control, including a reception area where visitors must report before accessing the controlled areas; and
  - Controlled access by employees and authorised third parties.
- 6.2.3. Network wiring and equipment rooms and cabinets must be locked when unattended with access limited only to authorised personnel (typically network support staff) and visitors escorted by such authorised personnel. Other network cabling and devices should likewise be physically secured where feasible. Core network facilities must have the date and time of all entry and departure recorded.
- 6.2.4. All office doors must remain locked after hours or when offices are unattended for a period of time.
- 6.2.5. Mobile storage devices must be stored securely when unattended.
- 6.2.6. For purposes of this Policy, appropriate secure storage methods include (i) a locking security cable attached directly to the device in question, such as laptops, (ii) storage in a locked cabinet or closet, or (iii) storage in a locked office.
- 6.2.7. Encrypting data stored on mobile devices, such as whole disk encryption on laptop computers, reduces the risk of a breach of data resulting from theft, loss, or unauthorised access. When Users travel with mobile storage devices or use them in public places, appropriate security precautions must be taken to prevent loss, theft, damage, or unauthorised access to such devices. This includes, at the discretion of the management of the Company, the use of tracking and recovery software on laptop computers.
- 6.3. Environmental security
- 6.3.1. The possible threat of the environment on Users, property, and information and technology resources and assets of the Company must be assessed on an annual basis, unless required more frequently in terms of any other policy of the Company.

Based on the outcome of the risk assessment, appropriate key controls must be implemented to mitigate the risk. Some potential risks include, without limitation:

- Water: areas where there is a risk of water damage due to flooding or bursting of geysers should be identified. Servers and other sensitive equipment that contain (i) Personal Information, and / or (ii) Confidential Information should be kept away from these areas.



- Electrical power: electrical power for servers hosting (i) Personal Information, and / or (ii) Confidential Information must be protected by uninterruptable power supplies to (i) ensure the continuity of services during power outages, and (ii) protect equipment from damage due to power irregularities. Systems hosting such information must also be protected with a standby power generator where reasonably possible.
- Natural disasters: all conceivable threats should be identified and mitigating controls should be put in place. An example of a control could be to install lightning equipment to prevent lightning from causing damage to the building that the Company occupies.

#### 6.4. Incident Management

- 6.4.1. An incident log of all physical and environmental breaches must be kept. The incident log must indicate the (i) type of incident, and (ii) action that has been taken by the Company to manage the incident.
- 6.4.2. Furthermore, a log of all evidence gathered during any investigation regarding the cause and damage sustained as a result of any physical or environmental threat must be kept and stored in a secure folder.

### 7. **RIGHTS RESERVED BY THE COMPANY**

The Company reserves the right to monitor, audit, screen, and preserve Company information as the Company deems necessary, in its sole discretion, in order to maintain compliance with this Policy and, by extension, all relevant provisions of POPIA. Any dissemination, unauthorised use or benefit from any Company information by a User in contravention of this Policy may result in disciplinary action being taken against such User by the Company. Furthermore, the use of any account or system in such a way that breaches any of the provisions of this Policy will be reported to the appropriate supervisor or manager within the Company, which may lead to further disciplinary action being taken.

### 8. **ENFORCEMENT AND POTENTIAL DISCIPLINARY ACTIONS**

Any violation of this Policy may result in disciplinary action being taken against the User in question. Such disciplinary action will be taken in accordance with the Company's applicable disciplinary code, and may include the (i) termination of employment in relation to employees of the Company, or (ii) cancellation or termination of contractual relations in the case of other Users, such as contractors or consultants. Notwithstanding the foregoing, should any authorised User fail to adhere to this policy, the individual will be dealt with as prescribed by the Company's disciplinary code and procedures.

## **9 POLICY AWARENESS AND UPDATE**

- 9.1. Training and awareness: The (i) requirement for, and (ii) a User's obligation in terms of, this Policy will be explained in detail in the Company's induction program, in the case of employees of the Company. Further training and additional awareness regarding the Policy will be offered from time to time by the Company. The Company will specifically make Users who are not employees of the Company aware of the Policy.
- 9.2. Dissemination: This Policy will be made available on the Company's network, intranet or similar portals.
- 9.3. Review: This Policy will be reviewed from time to time in order to ensure ongoing compliance with POPIA, but such revisions will take place at least annually. More frequent review may be required in response to (i) exceptional circumstances, (ii) organisational change, or (iii) relevant changes in legislation or guidance.

## Disaster Recovery Policy

Policy	Disaster Recovery Policy
Document No.	POL APP

### 1. **ROLES AND RESPONSIBILITIES**

The disaster recovery policy must be reviewed at least annually to assure its relevance, just as in the development of such a policy. A planning team that consists of upper management and personnel from the IT department, human resources, or other operations should be assembled to review the disaster policy. Roles and responsibilities of the planning team should be as follows:

- Perform an initial risk assessment to determine current information system's vulnerabilities.
- Perform an initial Company impact analysis to document and understand the interdependencies among Company processes and determine how the Company would be affected by an information systems outage.
- Take an inventory of information systems assets such as computer hardware, software, applications, and data.
- Identify single points of failure within the information systems infrastructure.
- Identify critical applications, systems, and data.
- Prioritize key Company functions.

### 2. **IMPLEMENTATION**

The Company's personnel will carry out the following procedures in the implementation of the disaster recovery policy:

- Setup and maintain offsite facilities for data backup storage and electronic vaulting as well as redundant and reliable standby systems if necessary.
- Ensure that critical applications, systems, and data are distributed among facilities that are reasonably easy to get to but not so close that they could be affected by the same disaster.
- Establish written policies, contracts, and service level agreements with third party hosting, collocation, telecommunications, and Internet service providers that facilitate prompt recovery and continuity.
- Create an incident response team that consists of information security, IT, marketing, HR, legal, and other relevant personnel.
- Define the roles and responsibilities of the incident response team.

- Obtain each incident response team member's contact information.
- Determine which methods the incident response team members will use to communicate in the event of a disaster.
- Create a public relations officer to assist with the effective handling of an incident.
- Assign a manager (such as an IT Manager or Information Officer) that has the responsibility and authority to make critical IT decisions.
- Develop testing standards.
- Document and distribute the disaster recovery plan.
- Distribute copies of the written plans to everyone involved and also store extra copies in an offsite, fireproof vault.

### 3. **ROLE AND RESPONSIBILITY OF I/O**

The following are on-going procedures that must be followed by employees and monitored by the Information Officer:

- Continuously perform data "back-ups", store at least weekly back-up offsite, and test those "back-ups" regularly for data integrity and reliability.
- Test plans at least annually, document and review the results, and update the plans as needed.
- Analyse plans on an on-going basis to ensure alignment with current Company objectives and requirements.
- Provide security awareness and disaster recovery education for all team members involved.
- Continuously update information security policies and network diagrams.
- Secure critical applications and data by patching known vulnerabilities with the latest fixes or software updates.
- Perform continuous computer vulnerability assessments and audits.

## **CONCLUSION**

*The amendments have been compiled with the objective of guiding the Practice to become compliant with the stipulations of the Protection of Personal Information Act, No 4 of 2013.*

### *Resolution*

*The following policies and amendments applicable to the Company have been discussed and implemented at a meeting between the Information Officer the company.*

### Queries and objections:

The details of the Information Officer are as follows:

- Name: Pieter Uys
- Telephone number: +27 82 448 9662
- Physical address: 309 Brooks Street, Menlo Park, 0181
- Mail: [pieter@kaimara.co.za](mailto:pieter@kaimara.co.za)

All questions and queries relating to personal information must be directed the Information Officer using the contact information listed above.

# PROTECTION OF ACCESS TO INFORMATION ACT (PAIA) OF 2000 MANUAL

in terms of Section 51 of the Promotion of Access to Information Act 2 of 2000  
and  
Section 17 of the Protection of Personal Information Act 4 of 2013

## KAIMARA (PTY) Ltd

*(Hereafter referred to as the Company)*

Company Name:	Kaimara (Pty) Ltd
Company Registration Number:	2018/419858/07
VAT Registration Number (if applicable):	454 025 3848
Physical Address:	309 Brooks Street, Menlo Park, 0181
Postal Address:	309 Brooks Street, Menlo Park, 0181
Company Telephone Number:	+27 82 448 9662
Name of Information Officer:	Pieter Uys
e-mail Address of Information Officer:	<a href="mailto:pieter@kaimara.co.za">pieter@kaimara.co.za</a>

*(This manual was prepared in accordance with Section 51 of the Promotion of Access to Information Act, 2000 and to address requirements of the Protection of Personal Information Act, 2013)*

### 1. BACKGROUND TO THE PROMOTION OF ACCESS TO INFORMATION ACT

On 9 March 2001, the Promotion of Access to Information Act, No. 2 of 2000 (PAIA) came into operation, giving effect to the Section 32(2) Constitutional right of access to information.

In terms of Section 51(1) of the Promotion of Access to Information Act (PAIA), all heads of private bodies are required to compile a manual that provides information regarding the subjects and categories of records held by such private bodies.

This document serves as the Company's information manual and provides reference to the records held by the Company and the process to request access to such records.

Where a request is made in terms of the PAIA, the Company is obliged to release the information, subject to applicable legislative requirements.

## 2. **DEFINITIONS AND INTERPRETATION**

Definitions	Interpretation
Conditions for lawful processing	Means the conditions for the lawful processing of Personal Information as fully set out in Chapter 3 of POPIA.
Company	Shall mean Kaimara (Pty) Ltd specified on the Title page of this document.
Constitution	Means The Constitution of the Republic of South Africa, 1996.
Customer	Refers to any natural or juristic person that received or receives services from the Company.
Data Subject	Has the meaning ascribed thereto in Section 1 of POPIA
Employees	Refers to any person who works for or provides services to or on behalf of the Company and receives or is entitled to receive remuneration and any other person who assists in carrying out or conducting the business of the Company.
Information Officer	Means the appointed Information Officer (as defined in Section 1 of PAIA) of the Company
Manual	Means this manual prepared in accordance with Section 51 of PAIA and Regulation 4(1) (d) of the POPIA Regulations.
PAIA	Promotion of Access to Information Act 2 of 2000.
Personal Information	Has the meaning ascribed thereto in Section 1 of POPIA.
POPIA	Means the Protection of Personal Information Act 4 of 2013.
POPIA Regulations	Means the regulations promulgated in terms of Section 112(2) of POPIA.
Private Body	Has the meaning ascribed thereto in Sections 1 of both PAIA and POPIA
Processing	Has the meaning ascribed thereto in Section 1 of POPIA.
Responsible Party	Has the meaning ascribed thereto in Section 1 of POPIA.

Record	Has the meaning ascribed thereto in Section 1 of PAIA and includes Personal Information
Requestor	Has the meaning ascribed thereto in Section 1 of PAIA.
Request for Access	Has the meaning ascribed thereto in Section 1 of PAIA.
SAHRC	Means the South African Human Rights Commission.

### 3. **PAIA**

PAIA commenced on the 9th of March 2001. The purpose of PAIA is to give effect to Section 32 of the Constitution, a fundamental right in the Bill of Rights, being the right of access to any information held by the state and any right held by any other person and that is required for the exercise of any rights.

Section 50 of PAIA states that where a request is made for the Company to release a record, the Company is obliged to release the record, except where PAIA expressly provides for the withholding of the record.

PAIA further sets out the required procedures to be followed by a requestor when making a Request for Access. Section 51 of PAIA further states that “all Private Bodies are required to compile an information manual” or PAIA Manual.

### 4. **POPIA**

The Purpose of POPIA is to give effect to Section 14 of The Constitution, “The Right to Privacy”, by protecting Personal Information and regulating the free flow and processing of Personal Information.

POPIA sets minimum conditions which the Company must comply with to ensure that all Personal Information is respected and protected.

### 5. **PURPOSE OF THE PAIA MANUAL**

The purpose of PAIA is to:

- Promote the right of access to information.
- Create a culture of transparency and accountability.
- Giving the right to information.
- Actively promote a society in which the people of South Africa have access to information.
- Enable the people of South Africa to exercise and protect their rights.

Section 9 of PAIA recognises that the right to access information cannot be unlimited:

- Limitations aimed at the reasonable protection of privacy.
- Commercial confidentiality.
- Effective, efficient, and good governance.



This PAIA Manual complies with the requirements of guidelines mentioned in Section 10 of PAIA. It recognises that the appointed Information Regulator will be responsible to regulate compliance with PAIA and POPIA.

## 6. **AVAILABILITY OF THE PAIA MANUAL**

A copy of this PAIA Manual is available to the public for inspection at the Company's premises or on request from the designated contact person referred to in this Manual.

This Manual is also available for inspection at the Company's offices free of charge.

## 7. **CONTACT DETAILS OF THE MANAGING DIRECTOR OF THE COMPANY [SECTION 51(1)(A)]**

Company Name:	Kaimara (Pty) Ltd
Company Registration Number:	2018/419858/07
VAT Registration Number (if applicable):	454 025 3848
Physical Address:	309 Brooks Street, Menlo Park, 0181
Postal Address:	309 Brooks Street, Menlo Park, 0181
Company Telephone Number:	+27 82 448 9662
Name of Information Officer:	Pieter Uys
e-mail Address of Information Officer:	<a href="mailto:pieter@kaimara.co.za">pieter@kaimara.co.za</a>

## 8. **THE INFORMATION OFFICER OF THE COMPANY [SECTION 51(1)(B)]**

PAIA prescribes the appointment of an Information Officer for the Company. The Information Officer is responsible to assess request for access to information. The CEO of the Company fulfils such a function in terms of PAIA Section 51.

The Information Officer appointed in terms of the PAIA also refers to the Information Officer as referred to in the POPIA of 2013. All request for information in terms of PAIA and POPIA must be addressed to the Information Officer.

## **9. CONTACT DETAILS OF THE INFORMATION OFFICER OF THE COMPANY**

Refer to Paragraph 7 supra

## **10. GUIDE OF SA HUMAN RIGHTS COMMISSION [SECTION 51(1) (B)]**

PAIA grants a requester access to records of the Company, 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 PAIA must be made in accordance with the prescribed procedures and at the rates provided. The forms and tariff are dealt with in paragraphs 6 and 7 of PAIA.

A Guide has been compiled in terms of Section 10 of PAIA by the Human Rights Commission. It contains information to assist a person wishing to exercise a constitutional right, in terms of PAIA. The Guide is available from the SAHRC as follows:

The South African Human Rights Commission: PAIA Unit

Physical Address: 29 Princess of Wales Terrace  
corner York and St. Andrews Streets  
Parktown

Postal address: Private Bag 2700  
Houghton  
2041

Telephone number: +27 (11) 877 3600

Fax number: +27 (11) 403 0625

E-mail: [PAIA@sahrc.org.za](mailto:PAIA@sahrc.org.za)

**Kindly note that the Information Regulator will replace the duties of the SAHRC as from 1 July 2021**

# 11. **CATEGORIES OF RECORDS AVAILABLE ONLY ON REQUEST TO ACCESS IN TERMS OF PAIA [SECTION 51(1) (E)]**

## **Records held by the Company.**

“Employee” or “Personnel” refers to any person who works for, or provides services to, or on behalf of the Company. This includes, directors, all permanent, temporary, and part-time staff, as well as contract workers.

This section serves as a reference to the categories of information that the Company holds. The information is classified and grouped according to records relating to the following subjects and categories:

CATEGORIES OF RECORDS	DOCUMENT TYPE
<b>Records relating to the form of practice and related matters</b>	Documents pertaining to an incorporated company as required by the Companies Act 71 of 2008, including, but not limited to the prescribed certificates, memorandum and articles of association, forms and registers of directors and shareholders, company rules, minute books, resolutions and shareholders’ agreements; Practice code number and related records
<b>Records relating to the registration of practitioners working at the practice</b>	Registration certificates related documents; Proof of payment of registration and annual fees professional bodies.
<b>Employment records</b>	Employment contracts; Conditions of employment and work place policies such as leave policies; Employment equity and skills development plans and reports; Salary register; Documents related to disciplinary proceedings, arbitration awards, CCMA (Commission for Conciliation, Mediation and Arbitration) and other legal cases; Expense accounts; Relevant tax records and information pertaining to employees; <i>Locum</i> contracts and related documents and records; Contracted staff lists
<b>Financial records</b>	Annual Financial Statements, including directors’ reports; auditor’s reports; Accounting Records; Bank statements; Invoices, statements, receipts and related documents
<b>Tax and VAT records</b>	Copies of tax returns and documents relating to income tax and VAT, including payments made and VAT registration
<b>Client records</b>	Records are kept in respect of all clients, which include their addresses, services rendered, costs and relevant financial arrangements
<b>Health and safety records</b>	Evacuation plan; Information related to the Health and Safety Committee / Officer; Health and safety incident reports
<b>Records related to property (movable and immovable)</b>	Finance and lease agreements; Asset register; Debenture register; Stock sheets; Delivery notes and orders; Sale agreements; Purchase agreements
<b>Other Agreements</b>	Information Technology (IT) agreements (software and hardware); Agreements concerning provision of services or materials; Agreements with contractors and suppliers;
<b>Records relating to legal processes</b>	Complaints, pleadings, briefs and other documents pertaining to any actual, pending or threatened litigation, arbitration or investigation; Settlement agreements; Legal opinions/advice
<b>Insurance records</b>	Insurance policies, including professional indemnity insurance, group personal accident and group life insurance policies and related records; Claims records

Note that the accessibility of the records may be subject to the grounds of refusal set out in this PAIA manual.

Records deemed confidential on the part of a third-party, will necessitate permission from the third - party concerned, in addition to normal requirements, before the Company will consider access.

## **12. RECORDS FREELY AVAILABLE TO THE PUBLIC**

The categories of records that are available without a person having to request access in terms of the Act are:

- Certain marketing information, adverts, and brochures
- Certain product information
- External media releases
- Public company records

Other non-confidential records, such as statutory records maintained at CIPC, may also be accessed without the need to submit a formal application, however, please note that an appointment to view such records will still have to be made with the Information Officer.

## **13. DESCRIPTION OF THE RECORDS WHICH ARE AVAILABLE IN ACCORDANCE WITH ANY OTHER LEGISLATION [SECTION 51(1) (D)]**

Where applicable to its operations, the Company also retains records and documents in terms of the legislation below.

Unless disclosure is prohibited in terms of legislation or otherwise, records that are required to be made available in terms of these Acts shall be made available for inspection. A request to access must be done in accordance with the prescriptions of PAIA. The daily operations of this Company areas of compliance inter alia: Business legislation (including all regulations issued in terms of such legislation):

- Basic Conditions of Employment Act No 75 of 1997 , Labour Relations Act No 66 of 1995, Occupational Health and Safety Act No. 85 of 1993 and other legislation commonly referred to as “Labour Law”
- Constitution of the Republic of South Africa 1996
- Companies Act No 71 of 2008
- Consumer Protection Act 68 of 2008
- Electronic Communications and Transactions Act 25 of 2002 (ECTA)
- The Cybercrimes Act 19 of 2020
- Promotion of Access of Information Act No 2 of 2000
- Income Tax Act 58 of 1962
- Value Added Tax Act No 89 of 1991

- South African Revenue Services Act 34 of 1997

Although we have used our best endeavours to supply a list of applicable legislation, it is possible that this list may be incomplete.

It is further recorded that the accessibility of documents and records may be subject to the grounds of refusal set out in this PAIA Manual.

#### **14. REQUEST FOR ACCESS TO A RECORD [SECTION 51(1) (E)]**

Please note that the successful completion and submission of an access request form does not automatically allow the requester access to the requested record. An application for access to a record is subject to certain limitations if the requested record falls within certain categories as specified in PAIA. If it is suspected that the requester has obtained access to records through the submission of materially false or misleading information, legal proceedings may be instituted against the requester.

##### **Completion of the Access Request Form**

To facilitate a timely response to requests for access, all requesters should take note of the following when completing the Access Request Form:

- An Access Request Form must be completed. This form must be in the prescribed format as defined in Form C of Annexure B as identified in Government Notice Number 187, Regulation 6. A copy of the request form is attached.
- Proof of identity is required to authenticate the identity of the requester. Therefore, in addition to the access form, requestors will be required to supply a copy of their identification document.
- Type or print in BLOCK LETTERS an answer to every question.
- If a question does not apply, state "N/A" in response to that question.
- If there is insufficient space on a printed form, additional information may be provided on an additional attached page.

##### **Please note:**

- In terms of the Act, the requester is required to provide sufficient detail on the request form to enable the Company to identify the record and the requester. The requester should also indicate the format access is required in.
- 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.
- If a request is made on behalf of another person, the requester must submit proof of the capacity in which the requester is making the request to the satisfaction of the Company.
- An application for access to information can be refused if the application does not comply with the procedural requirements of PAIA.
- The successful completion and submission of an access request form does not automatically allow the requestor access to the requested record.
- If the request is for access to a record that contains information about a third-party, the Company is obliged to contact the third-party to inform them of the request and to give

them an opportunity to respond. If the third party furnishes reasons for the support or denial of access, the Company will consider these reasons in determining whether access may be granted.

### **Submission of the Access Request Form**

- The completed Access Request Form together with a copy of the identity document must be submitted either via the mail or email and must be addressed to the contact person as indicated above.
- An initial request fee of R50.00 is payable on submission.
- This fee is not applicable to Personal Requesters, referring to any person seeking access to records that contain their personal information.

### **Payment of Fees**

- Payment details can be obtained from the contact person as indicated above and can be made by EFT (no credit card payments are accepted). Proof of payment must be supplied.
- The access fee must be paid prior to access being given to the requested record.
- If the request for access is successful an access fee may be required for the search, reproduction or preparation of the records and will be calculated based on the Prescribed Fees.
- If a deposit has been paid in respect of a request for access, which is refused, then the information officer concerned must repay the deposit to the requester.

### **Notification**

- The Company will, within 30 days of receipt of the request, decide whether to grant or decline the request and give notice with reasons (if required) to that effect.
- The 30-day period within which the Company must decide whether to grant or refuse the request, may be extended for a further period of not more than thirty days, if the request is for a large volume of information. Or the request requires a search for information held at another office of the Company and the information cannot reasonably be obtained within the original 30-day period. The Company will notify the requester in writing should an extension be sought.
- The Company will notify the requester in writing should an extension be sought.

### **Grounds for Refusal of Access to Records**

The main grounds for refusal of a request for information are:

- Mandatory protection of the privacy of a third-party who is a natural person, who would involve the unreasonable disclosure of personal information of that natural person.
- Mandatory protection of the commercial information of a third-party if the record contains:
  - Trade secrets of that party.
  - Financial, commercial, scientific, or technical information which disclosure could likely cause harm to the financial or commercial interests of that party.

- Information disclosed in confidence by a third-party to the Company if the disclosure could put that third party to a disadvantage in negotiations or commercial competition.
- Mandatory protection of confidential information of third-parties if it is protected in terms of any agreement.
- Mandatory protection of the safety of individuals and the protection of property.
- Mandatory protection of records which could be regarded as privileged in legal proceedings.
- The commercial activities of the Company which may include:
  - Trade secrets of the Company.
  - Financial, commercial, scientific, or technical information which disclosure could likely cause harm to the financial or commercial interests of the Company.

Note that the requester may lodge an application with the court against the Company's rejection of an application. For details on the procedure, please refer to Chapter 2 of Part 4 of the Act.

If the request of access is granted, the requester will be able to gain access to the requested records as soon as is reasonably possible but only after the access fees have been paid.

## **Fees**

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.

If the request is granted then further fees are payable for the search, reproduction, preparation and for any time that has exceeded the prescribed hours to search and prepare the record for disclosure.

## **Schedule of Fees**

The fee for a copy of the manual as contemplated in Regulation 9(2)(c) is R1,10 for every photocopy of an A4-size page or part thereof.

The fees for reproduction referred to in Regulation 11(1) are as follows:

- |     |   |        |
|-----|---|--------|
| (a) | For every photocopy of an A4-size page or part thereof  | R1,10  |
| (b) | For every printed copy of an A4-size page or part thereof held on a computer or in electronic or machine- readable form | R0,75  |
| (c) | For a copy in a computer-readable form on compact disc  | R70,00 |
| (d) | (i) For a transcription of visual images, for an A4-size page or part thereof   | R40,00 |
|     | (ii) For a copy of visual images  | R60,00 |
| (e) | (i) For a transcription of an audio record, for an A4-size page or part thereof   | R20,00 |
|     | (ii) For a copy of an audio record  | R30,00 |

The request fee payable by a requester, other than a personal requester, referred to in Regulation 11(2) is R50,00.

The access fees payable by a requester referred to in Regulation 11(3) are as follows:

(1)(a)	For every photocopy of an A4-size page or part thereof	R1,10
(b)	For every printed copy of an A4-size page or part thereof held on a computer or in electronic or machine- readable form	R0,75
(c)	For a copy in a computer-readable form on compact disc	R70,00
(d)	(i) For a transcription of visual images, for an A4-size	R40,00
	(ii) For a copy of visual images	R60,00
(e)	(i) For a transcription of an audio record, for an A4-size page or part thereof	R20,00
	(ii) For a copy of an audio record	R30,00

To search for and prepare the record for disclosure, R30,00 for each hour or part of an hour reasonably required for such search and preparation.

The actual postage is payable when a copy of a record must be posted to a requester.

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

## **15. REMEDIES AVAILABLE WHEN THE COMPANY REFUSES A REQUEST**

### **Internal Remedies**

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

### **External Remedies**

A requestor that is dissatisfied with the Information Officer's refusal to disclose information, may within 30 days of notification of the decision, may apply to a Court for relief.

A third-party dissatisfied with the Information Officer's decision to grant a request for information, may within 30 days of notification of the decision, apply to a Court for relief.

For purposes of PAIA, the Courts that have jurisdiction over these applications are the Constitutional Court, the High Court or another court of similar status and a Magistrate's Court.

## **16. UPDATING OF THE PAIA MANUAL**

The Company will update this PAIA Manual at such intervals as may be deemed necessary.



## 17 **RIGHTS RESERVED BY THE COMPANY**

The Company reserves the right to monitor, audit, screen, and preserve Company information as the Company deems necessary, to maintain compliance with these Policies and all relevant provisions of PAIA. Any distribution, unauthorised use, or benefit from Company information by an employee or user, in contravention of these Policies may result in disciplinary action being taken by the Company. The use of any system in such a way that breaches any of the provisions of these Policies, will be reported to the Information Officer at the Company, which may lead to further disciplinary action being taken.

## 18. **ENFORCEMENT AND POTENTIAL DISCIPLINARY ACTIONS**

Any violation of these Policies may result in disciplinary action being taken against the employee or user in question. Such disciplinary action will be taken in accordance with the Company's disciplinary code and may include the termination of employment for employees of the Company, or cancellation of contractual relations in the case of other users, such as contractors or consultants.

## 19. **POLICY AWARENESS AND UPDATE**

### **Training and awareness:**

The requirement for these Policies will be explained in detail in the Company's induction program, in the case of employees of the Company. Further training regarding these Policies will be offered from time to time by the Company. The Company will specifically make users who are not employees of the Company aware of these Policies.

### **Dissemination:**

These Policies will be made available on the Company's website, intranet, or notice boards.

### **Review:**

These Policies will be reviewed from time to time to ensure ongoing compliance with PAIA. Such revisions will take place at least annually.

## 20. **INTERNAL DOCUMENT APPROVAL**

Information Officer Name	Signature	Date
Pieter Uys		

## 22. PAIA FORMS



J750

REPUBLIC OF SOUTH AFRICA

**FORM A**  
**REQUEST FOR ACCESS TO RECORD OF PUBLIC BODY**  
 (Section 18(1) of the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000))  
 [Regulation 6]

**FOR DEPARTMENTAL USE**

Reference number: .....

Request received by ..... (state rank,  
 name and surname of information officer/deputy information officer) on ..... (date)  
 at ..... (place).

Request fee (if any): R .....

Deposit (if any): R .....

Access fee: R .....

.....  
 SIGNATURE OF INFORMATION OFFICER/DEPUTY INFORMATION OFFICER

**A. Particulars of public body**

The Information Officer/Deputy Information Officer

## FORM A: REQUEST FOR ACCESS TO RECORD OF PUBLIC BODY

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

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

Full names and surname: .....

Identity number: 

--	--	--	--	--	--	--	--	--	--	--	--	--	--

Postal address: .....

Telephone number: (.....) ..... Fax number: (.....) .....

E-mail address: .....

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

## C. Particulars of person on whose behalf request is made

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

Full names and surname: .....

Identity number: 

--	--	--	--	--	--	--	--	--	--	--	--	--	--

## D. Particulars of record

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

## 1. Description of record or relevant part of the record:

.....  
 .....

## FORM A: REQUEST FOR ACCESS TO RECORD OF PUBLIC BODY

2. Reference number, if available: .....

3. Any further particulars of record:

.....

.....

.....

.....

.....

## E. Fees

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

Reason for exemption from payment of fees:

.....

.....

.....

.....

## F. Form of access to record

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

Disability: \_\_\_\_\_ Form in which record is required: \_\_\_\_\_

Mark the appropriate box with an X.

## NOTES:

- (a) Compliance with your request for access in the specified form may depend on the form in which the record is available.
- (b) Access in the form requested may be refused in certain circumstances. In such a case you will be informed if access will be granted in another form.
- (c) The fee payable for access to the record, if any, will be determined partly by the form in which access is requested.

1. If the record is in written or printed form:

<input type="checkbox"/>	copy of record*	<input type="checkbox"/>	inspection of record	<input type="checkbox"/>	<input type="checkbox"/>
--------------------------	-----------------	--------------------------	----------------------	--------------------------	--------------------------

2. If record consists of visual images -  
(this includes photographs, slides, video recordings, computer-generated images, sketches, etc.):

<input type="checkbox"/>	view the images	<input type="checkbox"/>	copy of the images*	<input type="checkbox"/>	transcription of the images*	<input type="checkbox"/>
--------------------------	-----------------	--------------------------	---------------------	--------------------------	------------------------------	--------------------------

## FORM A: REQUEST FOR ACCESS TO RECORD OF PUBLIC BODY

3. If record consists of recorded words or information which can be reproduced in sound:					
	listen to the soundtrack (audio cassette)		transcription of soundtrack* (written or printed document)		
4. If record is held on computer or in an electronic or machine-readable form:					
	printed copy of record*		printed copy of information derived from the record*		copy in computer readable form* (stiffy or compact disc)
*If you requested a copy or transcription of a record (above), do you wish the copy or transcription to be posted to you? Postage is payable.				YES	NO
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.					
In which language would you prefer the record?					

## G. Notice of decision regarding request for access

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

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

.....

Signed at ..... this day ..... of ..... year .....

.....  
SIGNATURE OF REQUESTER /  
PERSON ON WHOSE BEHALF REQUEST IS MADE

J751



REPUBLIC OF SOUTH AFRICA

**FORM B**  
**NOTICE OF INTERNAL APPEAL**  
 (Section 75 of the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000))  
 [Regulation 8]

STATE YOUR REFERENCE NUMBER: .....

**A. Particulars of public body**

The Information Officer/Deputy Information Officer:

**B. Particulars of requester/third party who lodges the internal appeal**

- (a) The particulars of the person who lodge the internal appeal must be given below.  
 (b) Proof of the capacity in which appeal is lodged, if applicable, must be attached.  
 (c) If the appellant is a third person and not the person who originally requested the information, the particulars of the requester must be given at C below.

Full names and surname: .....

Identity number: 

--	--	--	--	--	--	--	--	--	--	--	--	--	--

Postal address: .....

Telephone number: (.....) ..... Fax number: (.....) .....

E-mail address: .....

Capacity in which an internal appeal on behalf of another person is lodged:

Department of Justice and Constitutional Development

## FORM B: NOTICE OF INTERNAL APPEAL

**C. Particulars of requester**

This section must be completed ONLY if a third party (other than the requester) lodges the internal appeal.

Full names and surname: .....

Identity number: 

--	--	--	--	--	--	--	--	--	--	--	--	--	--

**D. The decision against which the internal appeal is lodged**

Mark the decision against which the internal appeal is lodged with an X in the appropriate box:

	Refusal of request for access
	Decision regarding fees prescribed in terms of section 22 of the Act
	Decision regarding the extension of the period within which the request must be dealt with in terms of section 28(1) of the Act
	Decision in terms of section 29(3) of the Act to refuse access in the form requested by the requester
	Decision to grant request for access

**E. Grounds for appeal**

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

State the grounds on which the internal appeal is based:

.....

.....

.....

.....

.....

State any other information that may be relevant in considering the appeal:

.....

.....

.....

.....

.....

.....

## FORM B: NOTICE OF INTERNAL APPEAL

## F. Notice of decision on appeal

You will be notified in writing of the decision on your internal appeal. If you wish to be informed in another manner, please specify the manner and provide the necessary particulars to enable compliance with your request.

State the manner: .....

Particulars of manner: .....

Signed at ..... this day ..... of ..... year.....

.....  
SIGNATURE OF APPELLANT

## FOR DEPARTMENTAL USE:

## OFFICIAL RECORD OF INTERNAL APPEAL:

Appeal received on ..... (date) by .....  
..... (state rank, name and surname of information officer/deputy information officer).

Appeal accompanied by the reasons for the information officer's/deputy information officer's decision and, where applicable, the particulars of any third party to whom or which the record relates, submitted by the information officer/deputy information officer on ..... (date) to the relevant authority.

OUTCOME OF APPEAL: .....

DECISION OF INFORMATION OFFICER/DEPUTY INFORMATION OFFICER CONFIRMED/NEW DECISION  
SUBSTITUTED

NEW DECISION: .....

DATE RELEVANT AUTHORITY .....

RECEIVED BY THE INFORMATION OFFICER/DEPUTY INFORMATION OFFICER FROM THE RELEVANT  
AUTHORITY ON (date): .....





J752

REPUBLIC OF SOUTH AFRICA

**FORM C**  
**REQUEST FOR ACCESS TO RECORD OF PRIVATE BODY**  
 (Section 53(1) of the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000))  
 [Regulation 10]

**A. Particulars of private body**

The Head:

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

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

Full names and surname: .....

Identity number: 

--	--	--	--	--	--	--	--	--	--	--	--	--	--

Postal address: .....

Telephone number: (.....) ..... Fax number: (.....) .....

E-mail address: .....

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

**C. Particulars of person on whose behalf request is made**

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

Full names and surname: .....

Identity number: 

--	--	--	--	--	--	--	--	--	--	--	--	--	--

## FORM C: REQUEST FOR ACCESS TO RECORD OF PRIVATE BODY

## D. Particulars of record

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

## 1. Description of record or relevant part of the record:

.....

.....

.....

.....

## 2. Reference number, if available:

.....

.....

.....

.....

## 3. Any further particulars of record:

.....

.....

.....

.....

## E. Fees

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

## Reason for exemption from payment of fees:

.....

.....

.....

.....

.....

## FORM C: REQUEST FOR ACCESS TO RECORD OF PRIVATE BODY

## F. Form of access to record

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

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

<b>1. If the record is in written or printed form:</b>					
	copy of record*		inspection of record		
<b>2. If record consists of visual images - (this includes photographs, slides, video recordings, computer-generated images, sketches, etc.):</b>					
	view the images		copy of the images*		transcription of the images*
<b>3. If record consists of recorded words or information which can be reproduced in sound:</b>					
	listen to the soundtrack (audio cassette)		transcription of soundtrack* (written or printed document)		
<b>4. If record is held on computer or in an electronic or machine-readable form:</b>					
	printed copy of record*		printed copy of information derived from the record*		copy in computer readable form* (stiffy or compact disc)
*If you requested a copy or transcription of a record (above), do you wish the copy or transcription to be posted to you? Postage is payable.				YES	NO

## G. Particulars of right to be exercised or protected

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

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

.....

.....

.....

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

.....

.....

.....

FORM C: REQUEST FOR ACCESS TO RECORD OF PRIVATE BODY

H. Notice of decision regarding request for access

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

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

.....

Signed at ..... this day ..... of ..... year .....

.....  
SIGNATURE OF REQUESTER /  
PERSON ON WHOSE BEHALF REQUEST IS MADE



FORM D  
AUTOMATICALLY AVAILABLE RECORDS AND ACCESS TO SUCH RECORDS:  
(Section 15 of the Promotion of Access to Information Act, 2000 (Act 2 of 2000))  
[Regulation 5A]

<b>DESCRIPTION OF CATEGORY OF RECORDS AUTOMATICALLY AVAILABLE IN TERMS OF SECTION 15(1)(a) OF THE PROMOTION OF ACCESS TO INFORMATION ACT, 2000</b>	<b>MANNER OF ACCESS TO RECORDS (e.g. website) (SECTION 15(1)(b))</b>
<b>FOR INSPECTION IN TERMS OF SECTION 15(1)(a)(i):</b>	
<b>FOR PURCHASING IN TERMS OF SECTION 15(1)(a)(ii):</b>	
<b>FOR COPYING IN TERMS OF SECTION 15(1)(a)(iii):</b>	
<b>AVAILABLE FREE OF CHARGE IN TERMS OF SECTION 15(1)(a)(iii):</b>	

Department of Justice and Constitutional Development