



PROTECTION OF PERSONAL INFORMATION ACT

Disclaimer: This document is generic in nature and was compiled giving due consideration to pertinent regulatory requirements. This document is provided as a guideline only and any reliance by the user to achieve desired behaviour will be at the user's own risk. Moonstone Compliance (Pty) Ltd accepts no liability for any damages suffered or losses incurred arising from the use of this document.

Copyright: The content of this document is copyright of Moonstone Compliance (Pty) Ltd. All rights reserved. You may not, except with Moonstone's express written permission, distribute or commercially exploit the contents of this document.

CONTROL MEASURES

- Establish a Regulatory Risk & Compliance Management Framework for the organisation.
- Implement control measures (actions, activities, processes and/or procedures) that will provide reasonable assurance that the organisation's compliance obligations are met and that non-compliances are prevented, detected and corrected.
- Control measures must be periodically evaluated and tested to ensure their continuing effectiveness.

Action / Activity / Process / Procedure	Control Owner
Annual Review	JAMES BONNER / SAN-MARIE BOTHA
Information Officer	JAMES BONNER
Regional Information Officers	BRANCH MANAGERS
Deputy Information Officer	PAUL MYERS
POPI Audit	BRANCH MANAGERS / SAN-MARIE BOTHA
POPI Awareness Training	BRANCH MANAGERS / SAN-MARIE BOTHA

POLICY STATEMENT

- This policy forms part of the policy owner's internal business processes and procedures.
- Any reference to the "organisation" shall be interpreted to include the "policy owner".
- The organisation's governing body, its employees, volunteers, contractors, suppliers and any other persons acting on behalf of the organisation 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.

Last date Amended: 09 April 2021

Last amended by: San-marie Botha

1. INTRODUCTION

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

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

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

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

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

2. DEFINITIONS

2.1 Personal Information

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

- race, gender, sex, pregnancy, marital status, national or ethnic origin, colour, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language and birth of a person;
- information relating to the education or the medical, financial, criminal or employment history of the person;
- any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other assignment to the person;
- the biometric information of the person;
- the personal opinions, views or preferences of the person;
- correspondence sent by the person that is implicitly or explicitly or private or confidential in nature or further correspondence that would reveal the contents of the original correspondence;
- the views or opinions of another individual about the person;
- the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

2.2 Data Subject

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

2.3 Responsible Party

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

2.4 Operator

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

2.5 Information Officer

The Information Officer is responsible for ensuring the organisations compliance with POPIA.

Frontline's Information Officers are based regionally.

Action / Activity / Process / Procedure	Control Owner
Annual Review	JAMES BONNER / SAN-MARIE BOTHA
Information Officer	JAMES BONNER
Regional Information Officers	BRANCH MANAGERS
Deputy Information Officer	PAUL MYERS
POPI Audit	BRANCH MANAGERS / SAN-MARIE BOTHA
POPI Awareness Training	BRANCH MANAGERS / SAN-MARIE BOTHA

The head of the organisation will ultimately be responsible for the duties of the Information Officer and will oversee all the Deputy and Regional Information Officers above.

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

2.6 Processing

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

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

- dissemination by means of transmission, distribution or making available in any other form; OR
- merging, linking, as well as any restriction, degradation, erasure or destruction of information.

2.7 Record

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

Writing on any material;

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

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

Book, map, plan, graph or drawing;

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

2.8 Filing System

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

2.9 Unique Identifier

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

2.10 De-Identify

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

2.11 Re-Identify

In relation to personal information of a data subject, means to resurrect any information or which can be used by a reasonably foreseeable method to the data subject, or can be used or manipulated by a reasonably foreseeable method to identify the data subject.

2.12 Consent

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

2.13 Direct Marketing

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

- Promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; OR
- Requesting the data subject to make a donation of any kind for any reason.

2.14 Biometrics

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

3. POLICY PURPOSE

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

- Breaches of confidentiality. For instance, the organisation 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 organisation uses information relating to them.
- Reputational damage. For instance, the organisation could suffer a decline in shareholder value following an adverse event such as a computer hacker deleting the personal information held by the organisation.

This policy demonstrates the organisation'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 practice.
- By cultivating an organisational 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 business practices that will provide reasonable assurance that the rights of data subjects are protected and balanced with the legitimate business needs of the organisation.

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

4. POLICY APPLICATION

This policy and its guiding principles applies to:

- The organisation’s governing body
- All branches, business units and divisions of the organisation
- All employees and volunteers
- All contractors, suppliers and other persons acting on behalf of the organisation

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

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

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

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

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

5. RIGHTS OF DATA SUBJECTS

Where appropriate, the organisation will ensure that its clients and customers are made aware of the rights conferred upon them as data subjects.

The organisation will ensure that it gives effect to the following seven rights.

5.1 The Right to Access Personal Information

The organisation recognises that a data subject has the right to establish whether the organisation holds personal information related to him/her or it including the right to request access to that personal information.

An example of a “Personal Information Request Form” can be found under Annexure A.

5.2 The Right to have Personal Information Corrected or Deleted

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

5.3 The Right to Object to the Processing of Personal Information

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

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

5.4 The Right to Object to Direct Marketing

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

5.5 The Right to Complain to the Information Regulator

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

An example of a "POPI Complaint Form" can be found under Annexure B.

5.6 The Right to be Informed

The data subject has the right to be notified that his/her or its personal information is being collected by the organisation.

The data subject also has the right to be notified in any such situation where the organisation has reasonable grounds to believe that the personal information of the data subject has been accessed or acquired by an unauthorised person.

6. GENERAL GUIDING PRINCIPLES

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

6.1 Accountability

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

The organisation will ensure that the provisions of POPIA and the guiding principles outlined in this policy were complied with through the

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

6.2 Processing Limitation

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

- in a fair, lawful and non-excessive manner, and
- only with the informed consent of the data subject, and
- only for a specifically defined purpose.

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

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

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

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

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

6.3 Purpose Specification

All of the organisation's business units and operations must be informed by the principle of transparency.

The organisation will process personal information only for specific, explicitly defined and legitimate reasons. The organisation will inform data subjects of these reasons prior to collecting or recording the data subject's personal information.

6.4 Further Processing Limitation

Personal information will not be processed for a secondary purpose unless that processing is compatible with the original purpose.

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

6.5 Information Quality

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

The more important it is that the personal information be accurate.

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

6.6 Open Communication

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

The organisation will ensure that it establishes and maintains a “contact us” (customercare@frontlineum.co.za) facility, for instance via its website or through an electronic helpdesk, for data subjects who want to:

- Enquire whether the organisation holds related personal information, or
- Request access to related personal information, or
- Request the organisation to update or correct related personal information, or
- Make a complaint concerning the processing of personal information.

6.7 Security Safeguards

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

Please refer our IT Security Policy documents in this regard.

- IT Policy (For staff and for brokers)
- IT Back Up and Procedure
- Electronic Data and Cyber Security Policy
- Disaster Management & Data Recovery Policy

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

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

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

All new employees will be required to sign a "POPI - Employee Consent and Confidentiality" document containing contractual terms for the use and storage of employee information. Confidentiality clauses will also be included to reduce the risk of unauthorised disclosures of personal information for which the organisation is responsible.

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

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

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

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

We have SLA Confidentiality clauses with all our IT, Electronic Equipment providers (ITEC), Software systems for Operational use in Marketing, Claims and Underwriting (TIAL/VOLUME Watermark).

6.8 Data Subject Participation

A data subject may request the correction or deletion of his, her or its personal information held by the organisation.

The organisation will ensure that it provides a facility for data subjects who want to request the correction or deletion of their personal information. (customercare@frontlineum.co.za) or any request via the data subject's broker.

Where applicable, the organisation will include a link to unsubscribe from any of its electronic newsletters or related marketing activities.

7. INFORMATION OFFICERS

The organisation will appoint an Information Officer and where necessary, a Deputy Information Officer to assist the Information Officer.

The organisation's Information Officer is responsible for ensuring compliance with POPIA.

The matrix of the Information Officer and its deputies are noted above.

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

Where no Information Officer is appointed, the head of the organisation will assume the role of the Information Officer.

Consideration will be given on an annual basis to the re-appointment or replacement of the Information Officer and the re-appointment or replacement of any Deputy Information Officers.

Once appointed, the organisation will register the Information Officer with the South African Information Regulator established under POPIA prior to performing his or her duties.

An example of an "Information Officer Appointment Letter" can be found under Annexure F.

8. SPECIFIC DUTIES AND RESPONSIBILITIES

8.1 Governing Body

The organisation's governing body (Board of Directors) cannot delegate its accountability and is ultimately answerable for ensuring that the organisation meets its legal obligations in terms of POPIA.

The governing body may however delegate some of its responsibilities in terms of POPIA to management or other capable individuals.

The governing body is responsible for ensuring that:

- The organisation appoints an Information Officer, and where necessary, a Deputy Information Officer.
- All persons responsible for the processing of personal information on behalf of the organisation:
 - are appropriately trained and supervised to do so,
 - understand that they are contractually obligated to protect the personal information they come into contact with, and
 - are aware that a wilful or negligent breach of this policy's processes and procedures may lead to disciplinary action being taken against them.
- Data subjects who want to make enquires about their personal information are made aware of the procedure that needs to be followed should they wish to do so.
- The scheduling of a periodic POPI Audit in order to accurately assess and review the ways in which the organisation collects, holds, uses, shares, discloses, destroys and processes personal information.

8.2 Information Officer

The organisation's Information Officer is responsible for:

- 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.
- Ensuring that the organisation makes it convenient for data subjects who want to update their personal information or submit POPI related complaints to the organisation. 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.

- As well as these listed, please refer Addendum A which includes detailed responsibilities as legislated.

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

Designation of a Deputy Information Officer

- Section 17 of PAIA provides for the designation of a Deputy Information Officer of a public body, and section 56 of POPIA extends the designation of a Deputy Information Officer for a private body.
- A person designated as a Deputy Information Officer will have sufficient time, adequate resources and the financial means to devote to matters concerning POPIA and PAIA; the Deputy Information Officer is the highest management office within a Body.
- A Deputy Information Officer is accessible to everyone, particularly to a data subject in respect of POPIA or a requester, in terms of PAIA;
- A Deputy Information Officer is committed to have a reasonable understanding of POPIA and PAIA in order to execute his or her duties.
- A Deputy Information Officer is committed to have a reasonable understanding of the business operations and processes of a body.

Delegation of authority by an Information Officer to a Deputy Information Officer

- An Information Officer(s) of both a public or private body may¹⁷, subject to legislation and policies governing the employment of personnel of the
- body concerned, delegate any power or duty conferred or imposed on him or her to a Deputy Information Officer of that body.
- Only an employee of a body can be delegated as a Deputy Information Officer.
- The delegation referred to above must be in writing, using the template substantially similar to the attached Delegation of Authority, template "C".
- The delegation of any powers or duties and responsibilities to a Deputy Information Officer does not prohibit an Information Officer from exercising the powers or performing the duty that he or she has delegated to a Deputy Information Officer ;
- Any power, duties and responsibilities delegated to a Deputy Information Officer should be exercised or performed subject to such conditions as an Information Officer may consider necessary. Any conditions of delegation, as conferred on the Deputy Information Officer, should ensure that the body is as accessible as reasonably possible for data subjects or requesters.
- An Information Officer of a body must ensure that he or she reserves his or her rights in the aforesaid delegation to –
 - exercise the powers or to perform the duties and responsibilities concerned himself or herself; and
 - withdraw or amend the aforesaid delegation at any time.
- An Information Officer must be aware that any right or privilege acquired or any obligation or liability incurred as a result of a delegation of any powers, duties and responsibilities is not affected by any subsequent withdrawal or amendment of the decision to delegate.

- Depending of the circumstances of the case, the obligation or liability incurred as a result of any delegation of any powers, duties and responsibilities may be imposed on either the Information Officer or responsible party in so far as POPIA is concerned.
- To ensure a level of accountability by a delegated Deputy Information Officer, bodies are encouraged to ensure that such duties and responsibilities or any power delegated to a Deputy Information Officer is part of his or her job description.
- Despite the above-mentioned delegation of a Deputy Information Officer, an Information Officer retains the accountability and responsibility for the functions delegated to the Deputy Information Officer.

8.3 IT Manager (DAYLE NEEDS TO CONFIRM THIS)

The organisation's outsourced IT Manager is responsible for:

- Ensuring that the organisation's IT infrastructure, filing systems and any other devices used for processing personal information meet acceptable security standards.
- Ensuring that all electronically held personal information is kept only on designated drives and servers and uploaded only to approved Cloud computing services.
- Ensuring that servers containing personal information are sited in a secure location, away from the general office space.
- Ensuring that all electronically stored personal information is backed-up and tested on a regular basis.
- Ensuring that all back-ups containing personal information are protected from unauthorised access, accidental deletion and malicious hacking attempts.
- Ensuring that personal information being transferred electronically is encrypted
- Ensuring that all servers and computers containing personal information are protected by a firewall and the latest security software.
- Performing regular IT audits to ensure that the security of the organisation's hardware and software systems are functioning properly.
- Performing regular IT audits to verify whether electronically stored personal information has been accessed or acquired by any unauthorised persons.
- Performing a proper due diligence review prior to contracting with operators or any other third-party service providers to process personal information on the organisation's behalf. For instance, Cloud computing services.
- Process instructions received by relevant heads of department to remove users and their access to clients' personal information etc.
(When a staff member or broker leaves the system, external IT service provider must be instructed by the relevant heads of department to remove the user/s.)

8.4 Marketing & Communication DIRECTOR

The organisation's Marketing & Communication Manager is responsible for:

- Approving and maintaining the protection of personal information statements and disclaimers that are displayed on the organisation's website, including those attached to communications such as emails and electronic newsletters. Addressing any personal information protection queries from journalists or media outlets such as newspapers.
- Where necessary, working with persons acting on behalf of the organisation to ensure that any outsourced marketing initiatives comply with POPIA.

8.5 Employees and other Persons acting on behalf of the Organisation

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

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

Employees have restricted access on various platforms such as the Software Operational systems (such as TIAL – user profiles / VOLUME / COMPANY OPERATIONAL DOCUMENTS AND EMPLOYEE RECORDS)

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

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

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

- The data subject, or a competent person where the data subject is a child, consents to the processing; or
- The processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party; or
- The processing complies with an obligation imposed by law on the responsible party; or
- The processing protects a legitimate interest of the data subject; or

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

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

- Clearly understands why and for what purpose his, her or its personal information is being collected; and
- Has granted the organisation with explicit written or verbally recorded consent to process his, her or its personal information.

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

Informed consent is therefore when the data subject clearly understands for what purpose his, her or its personal information is needed and who it will be shared with.

Consent can be obtained in written form which includes any appropriate electronic medium that is accurately and readily reducible to printed form. Alternatively, the organisation will keep a voice recording of the data subject's consent in instances where transactions are concluded telephonically or via electronic video feed.

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

- the personal information has been made public, or
- where valid consent has been given to a third party, or
- the information is necessary for effective law enforcement.

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

- Process or have access to personal information where such processing or access is not a requirement to perform their respective work-related tasks or duties.
- Save copies of personal information directly to their own private computers, laptops or other mobile devices like tablets or smart phones. All personal information must be accessed and updated from the organisation's central database or a dedicated server.
- Share personal information informally. In particular, personal information should never be sent by email, as this form of communication is not secure. Where access to personal information is required, this may be requested from the relevant line manager or the Information Officer.

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

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

- Keeping all personal information that they come into contact with secure, by taking sensible precautions and following the guidelines outlined within this policy.
- Ensuring that personal information is held in as few places as is necessary. No unnecessary additional records, filing systems and data sets should therefore be created.
- Ensuring that personal information is encrypted prior to sending or sharing the information electronically. The IT Manager will assist employees and where required, other persons acting on behalf of the organisation, with the sending or sharing of personal information to or with authorised external persons.
- Ensuring that all computers, laptops and devices such as tablets, flash drives and smartphones that store personal information are password protected and never left unattended. Passwords must be changed regularly and may not be shared with unauthorised persons.
- Ensuring that their computer screens and other devices are switched off or locked when not in use or when away from their desks.
- Ensuring that where personal information is stored on removable storage medias such as external drives, CDs or DVDs that these are kept locked away securely when not being used.
- Ensuring that where personal information is stored on paper, that such hard copy records are kept in a secure place where unauthorised people cannot access it. For instance, in a locked drawer of a filing cabinet.
- Ensuring that where personal information has been printed out, that the paper printouts are not left unattended where unauthorised individuals could see or copy them. For instance, close to the printer.
- Taking reasonable steps to ensure that personal information is kept accurate and up to date. For instance, confirming a data subject's contact details when the client or customer phones or communicates via email. Where a data subject's information is found to be out of date, authorisation must first be obtained from the relevant line manager or the Information Officer to update the information accordingly.
- Taking reasonable steps to ensure that personal information is stored only for as long as it is needed or required in terms of the purpose for which it was originally collected. Where personal information is no longer required, authorisation must first be obtained from the relevant line manager or the Information Officer to delete or dispose of the personal information in the appropriate manner.

- Undergoing POPI Awareness training from time to time.

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

9. DATA CLASSIFICATION

The correct processing of data and encryption methods will be dependent on how various information is classified.

The following classification table assists in defining the various classification levels:

Data classification levels	Description	Examples
Public	All business data that's freely available to the public and that can't be leveraged to cause any financial loss, brand damage, or market share loss or jeopardise your clients, partners or employees.	Press releases, published annual reports, social media feeds, information on your public website.
Internal	Information that can be circulated only internally. Unauthorised disclosure of such information can lead to embarrassment and loss of competitive advantage.	Internal emails, project documents, training materials, organisational charts, policy guides. Internal procedures, policies and operational documents.
Confidential	Sensitive business data that if disclosed to unauthorised persons can harm a company, its customers, partners, or employees. Loss of confidential information may lead to regulatory backlashes.	Government identification numbers, employee pay stubs, customer information.
Restricted	Highly confidential information that can cause permanent damage to a company and its customers.	Strategic business plans, intellectual property (IP), trade secrets, undisclosed annual reports.

10. INTERNAL DATA PROCESSING ACCORDING TO CLASSIFICATION

Division	Types of documents handled	Data Classification
Marketing	Previous / Current Insurers Policy Schedules	Confidential
	Other Insurers quotations	
	Emails from brokers requesting quotations	Confidential
	Letters of appointment and or investigation	Confidential
	Broker Summaries	Confidential
	Proposal forms	Confidential
	Quotations / invoices from motor dealers	Confidential
	Our quotes with client information	Confidential
	Valuation certificates	Confidential
	Broker Training Assessments	Confidential
Statistical Data Reports	Confidential	
Underwriting	Broker instruction emails	Confidential

Last date Amended: 09 April 2021

Last amended by: San-Marie Botha

	<p>Broker appointments Cancellation letters from clients Cancellation letters to clients Confirmation of cover letters Proof of banking details Copy of ID documents Debit Order Authority forms Inventory forms Change of Risk Address Form Survey requests to OMI / External Surveyors Certificates of Insurance Underwriting Questionnaires Cross Border Cover Certificates Vehicle registration documents Policy documents sent to broker/clients Endorsement history for tax purposes Statistical data reports</p>	<p>Confidential Confidential Confidential Confidential Confidential Confidential Confidential Confidential Confidential Confidential Confidential Confidential Confidential Confidential Confidential Confidential Confidential Confidential Confidential</p>
Claims	<p>TransUnion checks Claim forms Rejection letters Settlement letters Authorisation forms Damage reports Assessor appointments and reports Bank statements Policy Schedules AR reports Copies of ID documents Copies of Driver licence Water accounts for claims Purchase invoices Valuations Quotations Contracts Registration certificates Vehicle license certificates Claims emails with personal information Claims Procedural Manual Statistical Data Reports</p>	<p>Confidential Confidential</p>
Salvage	<p>Personal information for Salvage matters Bank Statements Proof of residence Copies of ID documents Statistical Data Reports</p>	<p>Confidential Confidential Confidential Confidential Confidential</p>
Administration	<p>Marketing Material Staff Personnel records Quotations Company documents Company Policies Agreements Company insurance policies Minutes of Director meetings Payroll information Group Retirement and Staff Benefits records</p>	<p>Public Restricted Internal Restricted Internal / Confidential Restricted Restricted Internal / Confidential Confidential Confidential</p>

Finance	Financial transactions Financial records Finance Policies & Procedures Invoices Banking details Broker Agreements & Agency applications Broker Commissions / statements Bank Reconciliations Statistical Data Reports	Internal Confidential Internal Confidential Confidential / Internal Confidential Confidential / Internal Confidential / Internal Confidential
---------	---	---

Public Classification

Public data may be sent freely to external and internal persons as it is already part of the public domain. No encryption is necessary when sending such information.

Internal Classification

Documents classified under “Internal” may only be circulated internally within the organisation for the purposes for which it was intended. All our dealings with our Insurer will be considered as “internal” as we manage their policies and claims as part of our Binder Agreement with them.

It is required that Internal Confidential information must be encrypted when sending /distributing such information when classified as Confidential /Restricted under the Groups Administration and Finance above.

Confidential Classification

Sensitive business data or personal information may be shared internally to authorised or relevant employees for purposes for which the data is intended only. Encryption will be required for internal sharing of information if it is classified as Confidential/Restricted under the Group Administration and Finance. Should confidential information be communicated externally, encryption of electronic communications will apply and the external party will be required to sign a confidentiality agreement before receiving the sensitive data.

Restricted Classification

Restricted information may be shared internally to authorised or relevant employees for purposes for which the data is intended only.

All parties handling highly confidential restricted information are required to obtain permission from the Information Officer before sending internally/externally or alternatively the recipient to which the data is being sent, is required to sign a confidentiality agreement before release of the information. Email communications between the organisation and an external party are to be encrypted.

11. ENCRYPTION

Encryption will be incorporated into our daily operations as follows:

- All documentation and information that has been classified as Confidential and Restricted will be encrypted (see Data Classification)
- All communication/documentation containing Personal Information sent by employees from software systems and paperless document systems are and will be encrypted when distributed to external parties.
- All communication /documentation (such as Word, Excel & PDF, JPEG or any other related format) extracted from an employee’s computer data basis and sent via

Email channels, will be encrypted by means of a procedure to secure such document attachments containing Personal Information.

- No email communication will have Personal Information of clients in the body of the email nor in the subject line of any email sent out to external parties.
- All Personal information sent out to external parties will be encrypted by utilising a separate document obtained from the system (TIAL/VOLUME/Personal Computer database/External drives, CD's or DVD's, memory sticks) and we will secure the said document with password protection/mechanism.
- The encryption process and mechanism are addressed in a separate document, named "Secure Your Document" in explanation of how to secure various formats of documentation.

12. POPI AUDIT

The organisation's Information Officer will schedule periodic POPI Audits.

The purpose of a POPI audit is to:

- Identify the processes used to collect, record, store, disseminate and destroy personal information.
- Determine the flow of personal information throughout the organisation. For instance, the organisation's various business units, divisions, branches and other associated organisations.
- Redefine the purpose for gathering and processing personal information.
- Ensure that the processing parameters are still adequately limited.
- Ensure that new data subjects are made aware of the processing of their personal information.
- Re-establish the rationale for any further processing where information is received via a third party.
- Verify the quality and security of personal information.
- Monitor the extent of compliance with POPIA and this policy.
- Monitor the effectiveness of internal controls established to manage the organisation's POPI related compliance risk.

In performing the POPI Audit, Information Officers will liaise with line managers in order to identify areas within in the organisation's operation that are most vulnerable or susceptible to the unlawful processing of personal information.

Information Officers will be permitted direct access to and have demonstrable support from line managers and the organisation's governing body in performing their duties.

13. AUDIT CHECKPOINTS

8 conditions for lawfully processing of information

<p>1. Accountability</p> <p>The responsible party must ensure that the conditions and all the measures set out in the Act that give effect to such conditions, are complied with at the time of the determining the purpose and means of the processing.</p>	<p>Questions to ask:</p> <p>Who will be tasked with the responsibility of compliance in your organisation? <i>This individual will be held liable for non-compliance in certain situations.</i></p> <p>How will this individual ensure the organisation is POPI compliant? <i>Policies and procedures must be in place.</i></p>
<p>2. Processing Limitation</p> <p>Personal information may only be processed in a fair and lawful manner and only with the consent of the data subject.</p>	<p>Questions to ask:</p> <p>Was the personal information obtained directly from the Data Subject? <i>One of the requirements of the Act is that any personal information must be obtained directly from the Data Subject.</i></p> <p>Is the Data Subject aware that you have gathered his/her information and consented to the information being used? <i>Consent from the Data Subject is essential before gathering or processing any personal information.</i></p> <p>If the personal information has been gathered from a third party, has the Data Subject consented to this information being shared and used by you? <i>This is a requirement.</i></p> <p>Is the amount of information being gathered excessive? <i>Only information that is required for the specific purpose for which it is gathered may be stored. You may collect more information than required for the intended purpose for future use if you obtain the necessary consent from the Data Subject (this is regarded as "Further Processing" in the Act.</i></p>
<p>3. Purpose Specific</p> <p>Personal information may only be processed for specific, explicitly defined and legitimate reasons.</p>	<p>Questions to ask:</p> <p>For what specific, explicit and lawful purpose is the personal information being collected? <i>This purpose must be documented and adhered to.</i></p> <p>Is the Data Subject aware of the purpose for which the data has been collected? <i>Data Subject has the right to know what information you have and for what purpose it was gathered.</i></p> <p>Can you link all personal information collected to legitimate reasons for collecting? <i>Personal information only to be gathered for specific, explicit and lawful purposes.</i></p> <p>For what time period may you retain specific personal information? <i>Personal information may only be used for the specific purpose for which it was gathered and thereafter it must be destroyed. This procedure should be covered in the POPIA policies and procedures manual.</i></p> <p>How will you keep track of when personal information must be destroyed? <i>You will be required to account for what information you hold, for what purpose it was gathered and a date that that information must be destroyed.</i></p> <p>What process will be used to destroy Personal Information, in a manner that prevents its reconstruction, after you are no longer authorized to retain such records? <i>This is an essential step in the process. This procedure should be covered in the POPIA policies and procedures manual.</i></p>
<p>4. Further Processing Limitation</p> <p>Personal information may not be processed for a secondary purpose unless that processing is compatible with the original</p>	<p>Questions to ask:</p> <p>If you intend to reuse personal information is it in accordance and compatible with the purpose for which it was collected? <i>Should you want to use existing personal information for any other purpose other than what the information was gathered for, confirmation will be required from the Data Subject again.</i></p> <p>Is the Data Subject aware of the continued use of their personal information?</p>

Last date Amended: 09 April 2021

Last amended by: San-Marie Botha

purpose.	<i>When gathering information, you have to advise the Data Subject what the information will be used for and for what period you will hold that information.</i>
<p>5. Information Quality</p> <p>The responsible party must take reasonable steps to ensure that the personal information collected is complete, accurate, not misleading and updated where necessary.</p>	<p>Questions to ask:</p> <p>How do you ensure that personal information is reliable and accurate at all times? <i>By obtaining information directly from the data source, accuracy is more probable. It is always advisable to validate the personal information as it is being captured. If it is not possible for the data subject to input their own information, or if the information is captured from one format to another (i.e. from a paper form to an IT system, then the information should be sent to the data subject for validation.</i></p> <p>What process do you have in place to allow Data Subjects to update their information or withdraw consent? <i>When advising Data Subjects of the information you hold and for what purpose you hold it, they must be given details of how to update their information or withdraw consent. This procedure should be covered in the POPIA policies and procedures manual. It is advisable to develop procedures for automatically checking the accuracy of information on a regular basis, but sending a validation request to the data subjects.</i></p>
<p>6. Openness</p> <p>The data subject whose information you are collecting must be aware that you are collecting such personal information and for what purpose the information will be used.</p>	<p>Questions to ask:</p> <p>How do you gather personal information from Data Subjects and what process do you have in place to get consent for collecting and using personal information? <i>This is an important step and proof of consent is essential.</i></p> <p>How do you inform the Data Subject of the purpose for which the information is being gathered? <i>The Data Subject must be informed of how the data will be used at the time of gathering the information.</i></p> <p>What evidence do you have that Data Subjects have consented to the collection of their personal information? <i>Proof of consent must be retained to safeguard you against claims of misuse made by the Data Subject.</i></p> <p>Does the Data Subject know who the responsible party is in your organization? <i>When gathering information, Data Subjects must be given the details of the responsible person in your organization including contact details.</i></p> <p>How do you inform the Data Subjects of their right to lodge a complaint with the Information Regulator? <i>At the time that the personal information is gathered, the Data Subject must be advised of his/her rights to complain to the Information Regulator if misuse is suspected. The Information Regulator's information and contact details must be provided to the Data Subject.</i></p> <p>Have you advised the Data Subject of his/her rights to access his/her information and to object to the processing of said information? <i>This is a requirement.</i></p>
<p>7. Security Safeguards</p> <p>Personal information must be kept secure against the risk of loss, unlawful access, interference, modification, unauthorized destruction and disclosure.</p>	<p>Questions to ask:</p> <p>What procedure do you have in place to identify any foreseeable internal and external risks to personal information? <i>A safety and security risk assessment is required.</i></p> <p>What processes do you have in place to prevent personal information from falling into unauthorized hands? <i>Strict adherence to safety and security policies must be enforced. This procedure should be covered in the POPIA policies and procedures manual.</i></p> <p>What procedure do you have in place to establish and maintain appropriate safeguards against the identified risks? <i>The responsible person must enforce strict policies and procedures to safeguard personal information in your possession. This procedure should be covered in the POPIA policies and procedures manual.</i></p> <p>How do you determine which employees are permitted access personal information and what information they are permitted to access? <i>Strict policies and procedures are required regarding who has access, and how they gain access, to the personal information in your possession. This procedure</i></p>

	<p><i>should be covered in the POPIA policies and procedures manual.</i></p> <p>What processes do you have in place to alert you when personal information is accessed or modified without authorization? <i>This procedure should be covered in the POPIA policies and procedures manual.</i></p> <p>What processes do you have in place to identify the source of a data breach and the procedure to follow to neutralize such breach? <i>This procedure should be covered in the POPIA policies and procedures manual.</i></p> <p>What process do you have in place to ensure that safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards? <i>This procedure should be covered in the POPIA policies and procedures manual. It is the duty of the Responsible Person to ensure this process is followed.</i></p> <p>What processes do you have in place to prevent the reoccurrence of a data breach? <i>This procedure should be covered in the POPIA policies and procedures manual. It is the duty of the Responsible Person to ensure this process is followed.</i></p> <p>What procedure is to be followed when sharing personal information with an external operator? <i>A responsible party must, in terms of a written contract between the responsible party and the operator, ensure that the operator establishes and maintains the required security measures. The operator must advise immediately if there is the possibility that personal data has been accessed or acquired by any unauthorized person.</i></p> <p>What procedure is in place to inform the Data Subject that their personal information has been compromised? <i>The Data Subject must be advised via e-mail or in writing immediately if it is suspected that their personal information has been access by unauthorized persons. Sufficient information must be provided to allow the Data Subject to put measures in place to safeguard themselves against potential consequences of the security compromise. This procedure should be covered in the POPIA policies and procedures manual.</i></p> <p>What procedure is in place to inform the Information Regulator of any security breach? <i>The Information Regulator must be informed in the event of a security breach where personal information could be compromised. This procedure should be covered in the POPIA policies and procedures manual. It is the duty of the Responsible Person to ensure this process is followed.</i></p>
<p>8. Data Subject Participation</p> <p>Data subjects may request whether their personal information is held, as well as the correction and/or deletion of any personal information held about them.</p>	<p>Questions to ask:</p> <p>What are the Data Subject's rights regarding access to information being held by you? <i>Data Subjects may request information from you on whether you are holding their personal information. This request may not be declined and may not be charged for. The full nature and details of the information being held must also be provided on request but a charge may be levied for this information.</i></p> <p>What processes do you have in place to ensure such a request from a Data Subject is adhered to? <i>This procedure should be covered in the POPIA policies and procedures manual. It is the duty of the Responsible Person to ensure this process is followed.</i></p> <p>What processes do you have in place to allow Data Subjects to correct personal information that you hold or withdraw consent to use such information? <i>The Data Subject has the right to correct the personal information that you hold. They also have the right to withdraw consent at any time. This procedure should be covered in the POPIA policies and procedures manual.</i></p>

14. REQUEST TO ACCESS PERSONAL INFORMATION PROCEDURE

Data subjects have the right to:

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

- Request access to their personal information.
- Be informed how to keep their personal information up to date.

Access to information requests can be made by email, addressed to the Information Officer. The Information Officer will provide the data subject with a “Personal Information Request Form”.

Once the completed form has been received, the Information Officer will verify the identity of the data subject prior to handing over any personal information. All requests will be processed and considered against the organisation’s PAIA Policy.

The Information Officer will process all requests within a reasonable time.

POPI COMPLAINTS PROCEDURE

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

- POPI complaints must be submitted to the organisation in writing. Where so required, the Information Officer will provide the data subject with a “POPI Complaint Form”.
- Where the complaint has been received by any person other than the Information Officer, that person will ensure that the full details of the complaint reach the Information Officer within 1 working day.
- The Information Officer will provide the complainant with a written acknowledgement of receipt of the complaint within 2 working days.
- The Information Officer will carefully consider the complaint and address the complainant’s concerns in an amicable manner. In considering the complaint, the Information Officer will endeavour to resolve the complaint in a fair manner and in accordance with the principles outlined in POPIA.
- The Information Officer must also determine whether the complaint relates to an error or breach of confidentiality that has occurred and which may have a wider impact on the organisation’s data subjects.
- Where the Information Officer has reason to believe that the personal information of data subjects has been accessed or acquired by an unauthorised person, the Information Officer will consult with the organisation’s governing body where after the affected data subjects and the Information Regulator will be informed of this breach.
- The Information Officer will revert to the complainant with a proposed solution with the option of escalating the complaint to the organisation’s governing body within 7 working days of receipt of the complaint. In all instances, the organisation will provide reasons for any decisions taken and communicate any anticipated deviation from the specified timelines.

- The Information Officer's response to the data subject may comprise any of the following:
 - A suggested remedy for the complaint,
 - A dismissal of the complaint and the reasons as to why it was dismissed,
 - An apology (if applicable) and any disciplinary action that has been taken against any employees involved.
- Where the data subject is not satisfied with the Information Officer's suggested remedies, the data subject has the right to complain to the Information Regulator.
- The Information Officer will review the complaints process to assess the effectiveness of the procedure on a periodic basis and to improve the procedure where it is found wanting. The reason for any complaints will also be reviewed to ensure the avoidance of occurrences giving rise to POPI related complaints.

15. DISCIPLINARY ACTION

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

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

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

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

- A recommendation to commence with disciplinary action.
- A referral to appropriate law enforcement agencies for criminal investigation.
- Recovery of funds and assets in order to limit any prejudice or damages caused.

ANNEXURE A: PERSONAL INFORMATION REQUEST FORM

Please submit the completed form to the Information Officer:	
Name	
Contact Number	
Email Address	

Please be aware that we may require you to provide proof of identification prior to processing your request. There may also be a reasonable charge for providing copies of the information requested.

A. Particulars of Data Subject	
Name & Surname	
Identity Number:	
Postal Address:	
Contact Number	
Email Address	
B. Request	
I request the organisation to:	
(a) Inform me whether it holds any of my personal information	<input type="checkbox"/>
(b) Provide me with a record or description of my personal information	<input type="checkbox"/>
(c) Correct or update my personal information	<input type="checkbox"/>
(d) Destroy or delete a record of my personal information	<input type="checkbox"/>
C. Instructions	
D. Signature	
Signature	
Date	

ANNEXURE B: POPI COMPLAINT FORM

We are committed to safeguarding your privacy and the confidentiality of your personal information and are bound by the Protection of Personal Information Act.

Please submit your complaint to the Information Officer:	
Name	
Contact Number	
Email Address	

Where we are unable to resolve your complaint, to your satisfaction, you have the right to complain to the Information Regulator:

THE INFORMATION REGULATOR: MS MMAMOROKE MPHELO
PHYSICAL ADDRESS: SALU Building, 316 Thabo Sehume Street, Pretoria
EMAIL: infoereg@justice.gov.za
WEBSITE: <http://www.justice.gov.za/infoereg/index.html>

A. Particulars of Complainant	
Name & Surname	
Identity Number:	
Postal Address:	
Contact Number	
Email Address	
B. Details of Complaint	
C. Desired Outcome	
D. Signature	
Signature	
Date	

ANNEXURE C: POPI NOTICE AND CONSENT FORM

POPI NOTICE AND CONSENT FORM

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

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

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

Our Information Officer's Contact Details	
Name	
Contact Number	
Email Address	

Purpose for Processing your Information

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

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

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

Consent to Disclose and Share your Information

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

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

I hereby authorise and consent to the organisation sharing my personal information with the following persons:			
1.		2.	
3.		4.	
Signature		Date	

ANNEXURE D: EMPLOYEE CONSENT AND CONFIDENTIALITY CLAUSE

EMPLOYEE CONSENT AND CONFIDENTIALITY CLAUSE

- “Personal Information” (PI) shall mean the race, gender, sex, pregnancy, marital status, national or ethnic origin, colour, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language and birth of a person; information relating to the education or the medical, financial, criminal or employment history of the person; any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person; the biometric information of the person; the personal opinions, views or preferences of the person; correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence; the views or opinions of another individual about the person whether the information is recorded electronically or otherwise.
- “POPIA” shall mean the Protection of Personal Information Act 4 of 2013 as amended from time to time.
- The employer undertakes to process the PI of the employee only in accordance with the conditions of lawful processing as set out in terms of POPIA and in terms of the employer’s relevant policy available to the employee on request and only to the extent that it is necessary to discharge its obligations and to perform its functions as an employer and within the framework of the employment relationship and as required by South African law.
- The employee acknowledges that the collection of his/her PI is both necessary and requisite as a legal obligation, which falls within the scope of execution of the legal functions and obligations of the employer. The employee therefore irrevocably and unconditionally agrees:
 - That he/she is notified of the purpose and reason for the collection and processing of his or her PI insofar as it relates to the employer’s discharge of its obligations and to perform its functions as an employer.
 - That he/she consents and authorises the employer to undertake the collection, processing and further processing of the employee’s PI by the employer for the purposes of securing and further facilitating the employee’s employment with the employer.
 - Without derogating from the generality of the aforesaid, the employee consents to the employer’s collection and processing of PI pursuant to any of the employer’s Internet, Email and Interception policies in place insofar as PI of the employee is contained in relevant electronic communications.
 - To make available to the employer all necessary PI required by the employer for the purpose of securing and further facilitating the employee’s employment with the employer.
 - To absolve the employer from any liability in terms of POPIA for failing to obtain the employee’s consent or to notify the employee of the reason for the processing of any of the employee’s PI.
 - To the disclosure of his/her PI by the employer to any third party, where the employer has a legal or contractual duty to disclose such PI.
 - The employee further agrees to the disclosure of his/her PI for any reason enabling the employer to carry out or to comply with any business obligation the employer may have or to pursue a legitimate interest of the employer in order for the employer to perform its business on a day to day basis.
 - The employee authorises the employer to transfer his/her PI outside of the Republic of South Africa for any legitimate business purpose of the employer within the international community. The employer undertakes not to transfer or disclose his/her PI unless it is required for its legitimate business requirements and shall comply strictly with legislative stipulations in this regard.
- The employee acknowledges that during the course of the performance of his/her services, he/she may gain access to and become acquainted with the personal information of certain clients, suppliers and other employees. The employee will treat personal information as a confidential business asset and agrees to respect the privacy of clients, suppliers and other employees.
- To the extent that he/she is exposed to or insofar as PI of other employees or third parties are disclosed to him/her, the employee hereby agree to be bound by appropriate and legally binding confidentiality and non-usage obligations in relation to the PI of third parties or employees.

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

ANNEXURE E: SLA CONFIDENTIALITY CLAUSE

SERVICE LEVEL AGREEMENT CONFIDENTIALITY CLAUSE

- “Personal Information” (PI) shall mean the race, gender, sex, pregnancy, marital status, national or ethnic origin, colour, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language and birth of a person; information relating to the education or the medical, financial, criminal or employment history of the person; any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person; the biometric information of the person; the personal opinions, views or preferences of the person; correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence; the views or opinions of another individual about the person whether the information is recorded electronically or otherwise.
- “POPIA” shall mean the Protection of Personal Information Act 4 of 2013 as amended from time to time.
- The parties acknowledge that for the purposes of this agreement that the parties may come into contact with, or have access to PI and other information that may be classified, or deemed as private or confidential and for which the other party is responsible. Such PI may also be deemed or considered as private and confidential as it relates to any third party who may be directly or indirectly associated with this agreement. Further, it is acknowledged and agreed by the parties that they have the necessary consent to share or disclose the PI and that the information may have value.
- The parties agree that they will at all times comply with POPIA’s Regulations and Codes of Conduct and that it shall only collect, use and process PI it comes into contact with pursuant to this agreement in a lawful manner, and only to the extent required to execute the services, or to provide the goods and to perform their respective obligations in terms of this agreement.
- The parties agree that it shall put in place, and at all times maintain, appropriate physical, technological and contractual security measures to ensure the protection and confidentiality of PI that it, or its employees, its contractors or other authorised individuals comes into contact with pursuant to this agreement.
- Unless so required by law, the parties agree that it shall not disclose any PI as defined in POPIA to any third party without the prior written consent of the other party, and notwithstanding anything to the contrary contained herein, shall any party in no manner whatsoever transfer any PI out of the Republic of South Africa.

ANNEXURE F: INFORMATION OFFICER APPOINTMENT LETTER

INFORMATION OFFICER APPOINTMENT LETTER

I 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.
- Ensuring 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.
- Responsibilities shall include, legislated duties as per **ADDENDUM A**.

I hereby accept the appointment as Information Officer

Signature

Name & Surname

Date

Last date Amended: 09 April 2021

Last amended by: San-Marie Botha

ADDENDUM A: INFORMATION OFFICER DUTIES

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

1. Information Officer and Deputy Information Officer(s) to keep abreast of the latest developments in POPIA and PAIA.
2. The Information officer has an in depth understanding of the business operations and procedures of the body.
3. The encouragement of compliance by the Body with the conditions for the lawful processing of personal information.

For example:

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

- 1.1.2 dealing with requests made to the Body pursuant to POPIA.

For example-

1.1.2.1 an Information Officer of a Body will be expected to render such reasonable assistance, free of charge, as is necessary to enable the requester or data subject to comply with the prescribed process for submitting a request in terms of section 18 of PAIA5 and section 24 of POPIA. If a requester or data subject has made any request that does not comply with the requirements of PAIA or POPIA, the Information Officer concerned may not refuse the request because of that non-compliance, unless the Information Officer has:

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

- 1.3 working with the Regulator in relation to investigations conducted pursuant to Chapter 6 of POPIA in relation to the body.

For example-

1.1.3.1 the responsible party must obtain prior authorisation from the Regulator pertaining to the following-

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

- d) *transfer of 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 as referred to in section 727.*

1.1.3.2 pending the authorisation or completion of investigation by the Regulator, or until such time the responsible party receives a notice that a more detailed investigation will not be conducted, the responsible party is prohibited from carrying out information processing. This means that processing that falls under paragraph 6.1.3.1 above is suspended pending the authorisation from the Regulator.

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

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

- 1.2.1 a compliance framework is developed, implemented, monitored and maintained;
 - 1.2.2 a personal information impact assessment is done to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information;
 - 1.2.3 a manual is developed, monitored, maintained and made available as prescribed in sections 14 and 51 of PAIA, as amended;
 - 1.2.4 internal measures are developed together with adequate systems to process requests for information or access thereto;
 - 1.2.5 internal awareness sessions are conducted regarding the provisions of POPIA, regulations made in terms of POPIA, codes of conduct, or information obtained from the Regulator; and
 - 1.2.6 upon request by any person, copies of the manual are provided to that person upon the payment of a fee to be determined by the Regulator from time to time.
- 1.3 The Information Officer of each public Body must annually, and in terms of section 32 of PAIA, submit to the Regulator a report regarding-
- 1.3.1. the number of requests for access received;
 - 1.3.2. the number of requests for access granted in full;
 - 1.3.3. the number of requests for access granted in terms of section 46 of PAIA;
 - 1.3.4. the number of requests for access refused in full and refused partially and the number of times each provision of PAIA was relied on to refuse access in full or partially;
 - 1.3.5. the number of cases in which the periods stipulated in section 25(1) of PAIA were extended in terms of section 26 (1) of PAIA;
 - 1.3.6. the number of internal appeals lodged with the relevant authority and the number of cases in which, as a result of an internal appeal, access was given to a record;
 - 1.3.7. the number of internal appeals which were lodged on the ground that a request for access was regarded as having been refused in terms of section 27 of PAIA;
 - 1.3.8. the number of applications to a court which were lodged on the ground that an internal appeal was regarded as having been dismissed in terms of section 77 (7) of PAIA.