PROTECTION OF PERSONAL INFORMATION POLICY

Table of Contents

1. INTRODUCTION

1.1. The right to privacy is an elementary human right that is both recognised and protected in the South African Constitution as well as in the Protection of Personal Information Act 4 of 2013 ("PoPIA").

1.2. The aim of PoPIA is to promote the protection of privacy through providing a set of guiding principles that are intended to be used in a subtle manner when processing personal information.

1.3. When providing quality goods and/or services, the organisation is involved in the collection, use and disclosure of certain aspects of the personal information that is gathered from clients and/or customers and/or employees and/or other stakeholders.

1.4. A person's right to privacy necessitates them having control over their personal information and being able to conduct their affairs relatively free from unwanted interference.

1.5. In view of the importance of privacy, the organisation is committed to effectively managing all personal information in accordance with the provisions in PoPIA.

2. DEFINITIONS

2.1. "**Biometrics**" is a technique of personal identification that is based on physical and/or physiological and/or behavioural characterisation including (but not limited to): blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition.

2.2. "**Consent**" means that voluntary permission is given by the data subject, for the purpose of processing of personal information.

2.3. "**Data Subject**" is the client and/or customer and/or a company that supplies the organisation with services and/or products and/or any other goods.

2.4. "**De-Identify**" means to delete and/or destroy any information that identifies a data subject or which can be used by a reasonably foreseeable method to identify that data subject, or when linked to any other information, identifies the data subject.

2.5. "**Direct Marketing**" means to approach a data subject, either in person or by mail or by electronic communication, for the direct or indirect purpose of (but not limited to):

2.5.1. Promoting or offering to supply, in the ordinary course of business, any goods, products or services to the data subject; or

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

2.6. "**Filing System**" means any structured set of personal information details, whether centralised, decentralised or dispersed on a functional or geographical basis, which is stored and/or accessible according to specific criteria.

2.7. "**Information Officer**" or head of the organisation (where applicable) is responsible for ensuring that the organisation is compliant with PoPIA. Once appointed, the Information Officer must be registered with the South African Information Regulator established under PoPIA prior to performing their duties. Deputy Information Officers can also be appointed to assist the Information Officer where necessary.

2.8. "**Operator**" is the person who processes the personal information for a responsible party, being the organisation, in terms of a contract or a mandate. For example, a third-party service provider has been appointed

and contracted by the organisation to destroy documents that contain personal information. It is the responsibility of the third party to ensure that their operators and/or employees and/or contractors have an indemnity clause included in their contract or mandate.

2.9. "**Personal Information**" is defined as any information that can be used to identify a person although it can mean different things in different contexts. In the context of this policy Personal Information relates to an identifiable, living, natural person, or where applicable, an identifiable, existing juristic person (such as a company). It includes, (but is not limited) to information concerning:

2.9.1. race, gender, sex, pregnancy, marital status, nationality or ethnic origin, colour, sexual orientation, age, physical or mental health, disability, physically recognisable attributes, religion, conscience, belief, culture, language and birth information pertaining to an individual;

2.9.2. information relating to the education or the medical, financial, criminal or employment history of the individual;

2.9.3. any identifying number, symbol, email address, physical address, telephone and/or cell phone number, location information, online identifier or any other particular assignment to the individual;

2.9.4. the biometric information of the individual;

2.9.5. the personal opinions, views and/or or preferences of the individual;

2.9.6. correspondence sent by the individual that is implicitly or explicitly of a private or confidential nature or any further correspondence that may subsequently arise and that would reveal the contents of the original correspondence;

2.9.7. the views or opinions of any other person about the individual;

2.9.8. the name of the individual if it appears with other personal information that relates to the individual or if the disclosure of the name itself would reveal additional information about the individual.

2.10. "**Processing**" is defined as the act of processing information, this includes any activity or any set of operations, whether by manual or automatic means, that concerns any personal information and this includes (but is not limited to):

2.10.1. the collection and/or receipt and/or recording and/or organisation and/or, collation and/or storage and/or updating and/or modification and/or deletion and/or retrieval and/or alteration and/or consultation or use;

2.10.2. dissemination by means of transmission and/or distribution and/or circulation and/or making available in any other form; or

2.10.3. merging and/or linking, as well as any restriction and/or degradation and/or debasement and/or erasure and/or destruction of information.

2.11. "**Record**" means any recorded information, regardless of form or medium, including (but not limited to):

2.11.1. Writing on any material;

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

2.11.3. Labels, markings or other writing that may identify or describe anything of which it forms a part of, or to which it is attached by any means;

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

2.11.5. 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.

2.12. "**Re-Identify**" this pertains to personal information of a data subject, and it means, to resurrect or restore any information that has been de-identified or deleted or destroyed in any way, that may identify the data subject, or data that can be used or manipulated by any reasonably foreseeable method to identify the data subject.

2.13. "**Responsible Party**" is the entity that requires the personal information for a particular reason and it deals specifically with the purpose and the means for processing the personal information. In this particular instance the organisation, who is doing the processing of the personal information, is the responsible party.

2.14. "**Unique Identifier**" means any type of identifier that is assigned to a data subject that may be used by a responsible party for the purposes of the operations of a company and/or organisation that uniquely identifies that data subject in relation to that responsible party.

3. POLICY PURPOSE

3.1. The purpose of this policy is to protect the organisation from any reasonable compliance risks that may be associated with the protection of personal information which includes (but is not limited to):

3.1.1. Breach of confidentiality. For instance, the organisation could suffer a loss in revenue where it is found that the personal information of data subjects has been shared or disclosed inappropriately, whether intentionally or unintentionally.

3.1.2. Failing to offer choice. For example, all data subjects should be free to choose how and for what purpose the organisation uses their information or any information that may relate to them.

3.1.3. Reputational damage. For example, the organisation could suffer a decline in shareholder value following an adverse event such as (but not limited to), a computer hacker deleting or stealing the personal information held by the organisation.

3.2. This policy evidences the organisation's intent and commitment to protecting the privacy rights of data subjects in the following manner:

3.2.1. Through documenting the desired behaviour to ensure compliance with the provisions of PoPIA and Best Practice Requirements.

3.2.2. By ensuring that the organisational culture recognises privacy, as a valuable human right.

3.2.3. By developing and implementing internal controls for the purpose of managing the compliance risk associated with the protection of personal information and ensuring that all employees are not only fully trained up but also are aware of the severity of the risks.

3.2.4. By creating business practices that will not only provide reasonable assurance that the rights of data subjects are protected and balanced, but that the legitimate business needs of the organisation are also met.

3.2.5. 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 as well as those of the data subjects.

3.2.6. By raising awareness through training and providing guidance to all employees but especially those individuals who process personal information so that they can act confidently and consistently.

4. POLICY APPLICATION

4.1. This policy and its guiding principles applies (but is not limited) to:

4.1.1. The governing body of the organisation;

4.1.2. All branches, business units and divisions of the organisation;

4.1.3. All employees and volunteers;

4.1.4. All contractors, suppliers and other persons acting for and on behalf of the organisation.

4.2. The guiding principles must be applied in all situations and must be read, together 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).

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

4.3.1. A **PROCESSING** of **PERSONAL INFORMATION** entered into a **RECORD** by or for a **RESPONSIBLE PERSON** who is **DOMICILED** in South Africa.

4.4. PoPIA does not apply in situations where the processing of personal information:

4.4.1. is concluded in the course of purely personal or household activities; or

4.4.2. where personal information has been de-identified.

5. RIGHTS OF DATA SUBJECTS

5.1. Where applicable, the organisation will ensure that its clients and/or customers, data subjects, are made aware of the rights they are entitled to.

5.2. The organisation will ensure that data subjects will be given access to the following six rights:

5.2.1. <u>The Right to Access Personal Information</u>

5.2.1.1. The organisation acknowledges that a data subject has the right to establish whether the organisation holds personal information related to them including the right to request access to that personal information.

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

5.2.2. <u>The Right to have Personal Information Corrected and/or Deleted</u>

5.2.2.1. The data subject has the right to request, where necessary, that their personal information be corrected and/or deleted where the organisation is no longer authorised to retain the personal information.

5.2.3. The Right to Object to the Processing of Personal Information

5.2.3.1. The data subject has the right, on reasonable grounds, to object to the processing of their personal information.

5.2.3.2. In such circumstances, the organisation undertakes to give consideration to the request as it pertains to the requirements of PoPIA. The organisation may stop using and/or disclosing the data subject's personal information and will, therefore, be in compliance with any statutory and contractual record keeping requirements, also approve the destruction of the personal information.

5.2.4. The Right to Object to Direct Marketing

5.2.4.1. The data subject has the right to object, verbally or in writing, to the processing of their personal information for purposes of direct marketing through unsolicited electronic communications.

5.2.5. The Right to Complain to the Information Regulator

5.2.5.1. The data subject has the right to submit a complaint, in writing, to the Information Regulator regarding any alleged infringement of any of their rights protected under PoPIA and furthermore to institute civil proceedings regarding the alleged non-compliance with the protection of their personal information.

5.2.5.2. An example of a "POPIA Complaint Form" can be found under **ANNEXURE B**

5.2.6. The Right to be Informed

5.2.6.1. The data subject has the right to be notified, in writing or by electronic means, that their personal information is being collected by the organisation.

5.2.6.2. The data subject also has the right to be notified in any situation, in writing or by electronic means, 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

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

6.1.1. Accountability

6.1.1.1. Failure to comply with PoPIA regulations could potentially damage the organisation's reputation, and furthermore, the organisation could be exposed to a civil claim for damages. The protection of personal information is, therefore, the responsibility of everyone.

6.1.1.2. The provisions of PoPIA and the guiding principles outlined in this policy must be complied with through the desired behaviour as documented by the organisation. The organisation reserves the right to and may take any appropriate action that it deems necessary, should those individuals whose intentions and/or negligent actions and/or omissions fail to comply with the laid down principles and

responsibilities as documented in this policy. These 'appropriate' actions may result in disciplinary action, which may further result in dismissal.

6.1.2. Processing Limitation

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

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

6.1.2.1.2. only with the written and/or electronic consent of the data subject; and

6.1.2.1.3. only for the specifically defined purpose that it was intended for.

6.1.2.2. The organisation will inform the data subject, in writing, of the reasons for collecting their personal information and obtain their written and/or electronic consent prior to processing the personal information.

6.1.2.3. 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 recorded consent.

6.1.2.4. The organisation will under no circumstances distribute or share personal information between separate legal entities, or any 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.

6.1.2.5. The data subject must be informed of the possibility that their personal information will be shared, where applicable, with any other entities of the organisation's business and they must be provided with the reasons for doing so.

6.1.2.6. An example of a "PoPIA Notice and Consent Form" can be found under **ANNEXURE C**.

6.1.3. Purpose Specification

6.1.3.1. All of the organisation's business units and operations must be informed, in writing on the principle of transparency.

6.1.3.2. Personal information can only be processed for very specific, explicitly defined, and legitimate reasons. The organisation will inform data subjects, in writing and/or electronically, of these reasons for collecting and/or recording the data subject's personal information, prior to collection or recording.

6.1.4. Further Processing Limitation

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

6.1.4.2. In the instances where the personal information is required for a purpose that is not compatible with the original purpose, additional written and/or electronic

consent will be required from the data subject, before processing can take place.

6.1.5. Information Quality

6.1.5.1. The organisation will take reasonable steps to ensure that all personal information collected is complete, accurate and in no way misleading.

6.1.5.2. The organisation understands that the information collected must be accurately recorded as it is of the utmost importance that beneficiary details (on a life insurance policy for example) are correct and verified.

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

6.1.6. Open Communication

6.1.6.1. The organisation will take reasonable steps to ensure that data subjects are notified, and that they are at all times aware of, the fact that their personal information is being collected. This must include the purpose for which the information is being collected and processed as well.

6.1.6.2. The organisation will ensure that it establishes and maintains a “contact us” facility, for example via its website or through an electronic helpdesk or through a portal, for data subjects who want to:

6.1.6.2.1. Enquire whether the organisation holds their related personal information, or

6.1.6.2.2. Request access to their related personal information, or

6.1.6.2.3. Request the organisation to update or correct or delete their related personal information, or

6.1.6.2.4. Make a complaint concerning the processing of their personal information.

6.1.7. Security Safeguards

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

6.1.7.2. 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.

6.1.7.3. The organisation will continuously review its security controls and this will also include the implementation of regular testing of protocol. Relevant and current measures will also be put into place to combat cyber-

attacks on the organisation's IT network and infrastructure.

6.1.7.4. The organisation will ensure that all paper and electronic records comprising of personal information are securely stored and made accessible only to those individuals, who are authorised to have access.

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

6.1.7.6. All existing employees will, after the required consultation process has taken place, be required to sign an addendum to their employment. This will contain the relevant consent and confidentiality clauses, where applicable.

6.1.7.7. The organisation's operators and third-party service providers will also be required to enter into service level agreements with the organisation. Both parties will pledge their commitment to PoPIA and the lawful processing of any personal information pursuant to the agreement. Furthermore, it will be a requirement that all of their employees will also be required to sign an addendum to their employment contracts. This will also contain the relevant consent and confidentiality clauses, where applicable.

6.1.7.8. An example of "Employee Consent and Confidentiality Clause" for inclusion in the organisation's employment

contracts can be found under **ANNEXURE D: EMPLOYEE CONSENT & CONFIDENTIALITY CLAUSE**.

6.1.7.9. An example of an "SLA Confidentiality Clause" for inclusion in the organisation's service level agreements can be found under **ANNEXURE E: SLA CONFIDENTIALITY CLAUSE**.

6.1.8. Data Subject Participation

6.1.8.1. A data subject may request, in writing or by electronic means, the correction or deletion of their personal information held by the organisation.

6.1.8.2. The organisation will ensure that it provides a facility for data subjects who want to request the correction or deletion of their personal information and that all employees are made aware of and trained in this regard.

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

7. INFORMATION OFFICERS

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

7.2. The organisation's Information Officer and Deputy Information Officer (where applicable) will be responsible for ensuring all compliance with PoPIA.

7.3. 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 “Best Business” practice, particularly within larger organisations or listed companies.

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

7.5. Consideration will be given on an annual basis to the re-appointment or replacement of the Information Officer as well as the re-appointment or replacement of any Deputy Information Officers (where applicable).

7.6. Once appointed, the organisation will register the Information Officer and their relevant information, with the South African Information Regulator established under PoPIA prior to them performing their duties.

7.7. An example of an “Information Officer Appointment Letter” can be found under **ANNEXURE F: INFORMTION OFFICER APPOINTMENT LETTER**.

8. SPECIFIC DUTIES AND RESPONSIBILITIES

8.1. Governing Body

8.1.1. The organisation’s governing body cannot delegate its accountability and is ultimately answerable for ensuring that the organisation meets its legal obligations in terms of PoPIA.

8.1.2. The governing body may however delegate some of its responsibilities in terms of PoPIA to management and/or other capable individuals.

8.1.3. The governing body is responsible for ensuring that:

8.1.3.1. The organisation appoints an Information Officer, and where necessary, a Deputy Information Officer.

8.1.3.2. All persons responsible for the processing of personal information on behalf of the organisation, and they will ensure that they:

8.1.3.2.1. are appropriately trained and supervised to perform these duties;

8.1.3.2.2. understand that they are contractually obligated to protect the personal information that they come into contact with; and

8.1.3.2.3. are aware that a wilful or negligent breach of this policy's processes and procedures may lead to disciplinary action being taken against them and that furthermore they may be dismissed, should they be found guilty.

8.1.3.3. Data subjects who wish to make enquiries about their personal information are free to do so, provided that they follow laid down procedures.

8.1.3.4. The scheduling of a periodic PoPIA Audit in order to accurately assess and review the ways in which the organisation collects, holds, uses, shares, discloses, destroys and processes personal information, must be performed on a regular basis and at least annually.

8.2. Information Officer

8.2.1. The organisation's Information Officer is responsible for:

8.2.1.1. Ensuring that the organisation has reasonable compliance with the provision of PoPIA.

8.2.1.2. Keeping the governing body updated in writing, about the organisation's information protection responsibilities under PoPIA. For example, in the case of a security breach, the Information Officer must inform and advise the governing body of their obligations with respect to the PoPIA regulations.

8.2.1.3. Continually analysing privacy regulations and aligning them with the organisation's personal information processing procedures. This will include (but not be limited to), reviewing the organisation's information protection procedures and related policies and ensuring that these are updated where and when applicable.

8.2.1.4. Ensuring that PoPIA Audits are scheduled and conducted on a regular basis, but at least annually.

8.2.1.5. Ensuring that the organisation makes it convenient and simple for data subjects who want to update their personal information or submit PoPIA related complaints to the organisation. For example, maintaining a "contact us" facility on the organisation's website or portal.

8.2.1.6. Approving and updating 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, whilst

also adhering to and with the Basic Conditions of Employment Act and the Labour Relations Act.

8.2.1.7. Encouraging compliance with the processes required for the lawful processing of personal information, by ensuring that regular training on the requirements is undertaken by all employees, both old and new.

8.2.1.8. 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, by means of regular documented and/or electronic communications.

8.2.1.9. Organising and overseeing the regular awareness training of employees and other individuals involved in the processing of personal information, takes place on behalf of the organisation.

8.2.1.10. Addressing employees' and contractors' (where applicable) PoPIA related questions.

8.2.1.11. Addressing all PoPIA related requests and complaints made by the organisation's data subjects.

8.2.1.12. 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 applicable, with regard to any matters of concern.

8.2.2. The Deputy Information Officer will assist the Information Officer in performing their duties, where required and when necessary.

8.3. IT Manager

8.3.1. The organisation's IT Manager is responsible for:

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

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

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

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

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

8.3.1.6. Ensuring that personal information being transferred electronically is adequately and securely encrypted.

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

8.3.1.8. Performing regular, irregular, (but at least annually), IT audits to ensure that the security of the organisation's hardware and software systems are functioning properly.

8.3.1.9. Performing regular, irregular, (but at least annually), IT audits to verify whether electronically stored personal information has been accessed and/or acquired by any unauthorised persons.

8.3.1.10. 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 example, cloud computing services or data capturers.

8.4. Marketing & Communication Manager

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

8.4.1.1. Approving and maintaining the protection of personal information statements and ensuring that disclaimers that are displayed on the organisation's website, including (but not limited to) those attached to any and all communications such as emails and electronic newsletters.

8.4.1.2. Addressing any personal information protection queries from journalists or media outlets such as newspapers or newsroom reporters.

8.4.1.3. Where necessary, working with persons acting on behalf of the organisation to ensure that any outsourced marketing initiatives comply with all PoPIA requirements.

8.5. Employees and other Persons acting on behalf of the Organisation

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

8.5.2. This personal information is to be treated as a confidential business asset and the privacy of data subjects is to be respected and protected at all times.

8.5.3. Employees and other persons acting on behalf of the organisation may not directly or indirectly, use, disclose or make public, in any manner what-so-ever, to any person or third party, both 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, unless authorised in writing or by electronic means, to do so.

8.5.4. 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 anything relating to the protection of a data subject's personal information.

8.5.5. Employees and other persons acting on behalf of the organisation will only process personal information where (but not limited to):

8.5.5.1. The data subject, or a legal guardian where the data subject is a child or who is legally incapacitated, consents in writing to the processing; or

8.5.5.2. The processing is necessary in order to carry out actions that are required to complete a contract to which the data subject is a party; or

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

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

8.5.5.5. The processing is necessary for the legitimate undertaking of the organisation or of a third party to whom the information is supplied.

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

8.5.6.1. Clearly understands why and for what purpose, their personal information is being collected and processed by the organisation; and

8.5.6.2. Has given the organisation explicit written or verbally recorded consent to process their personal information.

8.5.7. Employees and other persons acting on behalf of the organisation will consequently, prior to processing any personal information, obtain a specific and an informed written or recorded, instruction

that gives permission from the data subject to process their personal information.

8.5.8. The data subject clearly has to understand the reason why their personal information is needed and who it will be shared with, if applicable.

8.5.9. Consent can be obtained in writing and/or in an appropriate electronic medium that can be printed out. 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.

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

8.5.10.1. the personal information has been made public, or

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

8.5.10.3. the information is necessary for effective law enforcement.

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

8.5.11.1. Process or have access to personal information that they do not require in order to perform their work-related tasks or duties.

8.5.11.2. 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.

8.5.11.3. Share personal information informally.

8.5.11.4. Share personal information 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.

8.5.11.5. Transfer personal information outside of South Africa without the express written and documented permission from the Information Officer.

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

8.5.12.1. Keeping all personal information that they come into contact with secure, by taking reasonable precautions and following the guidelines outlined in this policy.

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

8.5.12.3. Ensuring that personal information is securely 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 and/or with authorised external persons.

8.5.12.4. 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 on a regular, irregular basis and may not be shared with any unauthorised individuals.

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

8.5.12.6. Ensuring that where personal information is stored on removable storage mechanisms such (but not limited to) as external drives, CDs or DVDs that these are kept locked away securely when not being used.

8.5.12.7. Ensuring that where personal information is stored on paper, that such hard copy records are kept in a secure place where unauthorised individuals cannot access it. For example, in a locked drawer and/or a filing cabinet and/or securely locked archives.

8.5.12.8. 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.

8.5.12.9. Taking reasonable steps to ensure that personal information is kept accurate and up to date. For example, confirming a data subject's contact details when in communication with the customer by phone and/or e-mail. Should a data subject's information found to be out of date, authorisation must first be

obtained from the relevant line manager and/or the Information Officer to update the relevant information.

8.5.12.10. 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 and/or the Information Officer to archive and/or delete and/or dispose of the personal information in the appropriate manner.

8.5.12.11. Undergoing PoPIA Awareness training from time to time.

8.5.13. Where an employee, or a person acting on behalf of the organisation, becomes aware or suspicious of any security breach such as (but not limited to) unauthorised access, interference, modification, destruction or the unsanctioned disclosure of personal information, they must immediately report this event or suspicion to the Information Officer or the Deputy Information Officer.

9. POPIA AUDIT

9.1. The organisation's Information Officer will schedule periodic PoPIA Audits on at least, an annual basis.

9.2. The purpose of a PoPIA audit is to:

9.2.1. Identify the processes used to collect, record, store, delete and/or destroy personal information.

9.2.2. Determine the flow of personal information throughout the organisation. For example, the organisation's various business units, divisions, branches and other associated organisations, such as services providers etc.

9.2.3. Redefine, where applicable, the purpose for gathering and processing personal information.

9.2.4. Ensure that the processing parameters are still adequately limited and properly managed.

9.2.5. Ensure that new data subjects are made aware of the processing of their personal information, if this has not already been done.

9.2.6. Re-establish the reason(s) for any further processing where information is received via a third party.

9.2.7. Verify that the quality and security of personal information is properly maintained.

9.2.8. Verify that compliance with PoPIA and this policy is properly maintained.

9.2.9. Verify the effectiveness of internal controls established to manage the organisation's PoPIA related compliance risk and make recommendations where necessary and applicable.

9.3. In performing the PoPIA 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.

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

10. REQUEST TO ACCESS PERSONAL INFORMATION PROCEDURE

10.1. Data subjects have the right to:

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

10.1.2. Request access to their own, personal information.

10.1.3. Be informed on how, best to keep their personal information current.

10.2. 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".

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

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

11. POPIA COMPLAINTS PROCEDURE

11.1. 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 PoPIA related complaints in accordance with the following procedure:

11.1.1. PoPIA complaints must be submitted to the organisation in writing. Where required, the Information Officer will provide the data subject with a “PoPIA Complaint Form”.

11.1.2. Where the complaint has been received by any person other than the Information Officer, that person will ensure that the complaint reaches the Information Officer within 1 working day.

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

11.1.4. The Information Officer will carefully consider the complaint and address the complainant’s concerns in an amicable manner. The Information Officer will endeavour to resolve the complaint in a fair and reasonable manner and in accordance with the principles outlined in PoPIA.

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

11.1.6. 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. Thereafter, the affected data subjects and the Information Regulator will be informed of this breach in writing.

11.1.7. The Information Officer will revert to the complainant with a proposed solution, in writing, 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.

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

11.1.8.1. A suggested remedy for the complaint,

11.1.8.2. A dismissal of the complaint and the reasons as to why it was dismissed,

A written apology (if applicable) and any disciplinary action that has been taken against any employees, contractors or 3rd parties involved.

11.1.9. In the instances where the data subject is not satisfied with the Information Officer's suggested remedies, the data subject has the right to complain and to take the matter up with the Information Regulator.

11.1.10. 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 to be wanting. The reason for any complaints will also be reviewed to ensure the avoidance of occurrences giving rise to PoPIA related complaints.

12. DISCIPLINARY ACTION

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

12.2. In the case of ignorance or minor negligence, the organisation will undertake to provide further awareness training to the employee to ensure that this does not re-occur.

12.3. Any gross negligence or the wilful mismanagement of personal information, will be considered a serious form of misconduct which will result in disciplinary action being levied against the employee and this may further result in dismissal.

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

12.4.1. A recommendation to commence with disciplinary action.

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

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

ANNEXURE A

PERSONAL INFORMATION REQUEST FORM

Please submit the completed form to the Information Officer:

Name	
Contact	
E-mail	

Please be aware that we may require you to provide proof of identification prior to processing.

A. Particulars of Data Subject		
Full name		
Identity #		
Postal Address		
Contact #s		
E-mail		
B. Request		
I request the organisation to:		
(a) Inform me whether it holds any of my personal information.		
(b) Provide me with a record or description of my personal information		
(c) Correct or update my personal information		
(d) Destroy or delete a record of my personal information		
C. Instructions		
D. Signature Page		
Signature:		
Date:		

ANNEXURE B

PoPIA 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 (PoPIA)	
Please submit your complaint to the Information Officer.	
Name	
Contact	
E-mail	

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

A. Particulars of Complainant	
Full name	
Identity #	
Postal Address	
Contact #s	
E-mail	
B. Details of Complainant	

C. Desired Outcome
E. Signature Page
Signature:
Date:

ANNEXURE C

PoPIA NOTICE AND CONSENT FORM

We understand that your personal information is important to you and that you may be reluctant to disclose it. Your privacy is just as important to us and we are committed to safeguarding and processing your information in accordance with the law.

We also want to make sure that you understand how and why we process your information. If for any reason you think that your information is not processed correctly, or that your information is being used for something other than that it was originally intended, please contact our Information Officer.

You can request access to your information that we currently hold, at any time and if you think that we have obsolete incorrect information, please request us to update or correct it.

Our Information Officer's Contact Details

Name	
Contact	
E-mail	

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 (but not limited to):-

- Providing you with advice, products and services that suit your needs as requested by yourself;
- To verify your identity and to conduct credit reference searches;
- To issue, administer and manage your insurance policies (where insurance to your purchase of product or services is applicable);
- To process insurance claims and/or to take recovery action (where applicable);
- To notify you of new products, services and/or developments that may be of interest to you;
- To confirm, verify and/or update your details;
- To comply with any legal and regulatory requirements.

Some of your information that we hold may include, (but is not limited to) your forenames and surname, e-mail address, your home and/or postal address and/or physical address and other information such as (but not limited to) your title, birth date, gender, occupation, qualifications, past

employment, residency status, your investments, assets, liabilities, insurance, income, expenditure, family history, medical information, next of kin and your banking details (all of which are “if applicable”)

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 reasonable precautions to ensure that the 3rd Party will treat your information with the same level of respect and with the same protection as required by ourselves. Therefore, your information may be hosted on serves managed by a 3rd Party Service Provider, which may be located outside of South Africa.

I hereby authorise and consent to the organisation sharing my personal information with:
Name and Surname
Signature
Date

ANNEXURE D: EMPLOYEE CONSENT & CONFIDENTIALITY CLAUSE

EMPLOYEE CONSENT & CONFIDENTIALITY CLAUSE

- " Personal Information" (PI) refers to the race, gender, sex, marital status, national or ethnic origin, colour, sexual orientation, age, physical or mental health, disability, physical appearance, religion, conscience or belief culture, language, and birth of a person. It also pertains to any information relating to the medical, financial, criminal or employment history of the person; any identifying number and/or symbol, e-mail address, physical address, telephone and/or cell number, location information, online identifier or any other particular and/or specific assignment to the person; the biometric information of the employee; the personal opinions, views or preferences of the employee; correspondence sent by the employee that is specifically or implicitly of a private and/or confidential nature or further correspondence that would in any way reveal the contents of the original correspondence; the views or opinions of another individual about the person, whether or not the information is recorded electronically or documented or any other way in which it is communicated.

- "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 current policy, which is also available to all employees on request and only to the extent that it is necessary to discharge its obligations and to perform its functions as an employer as it is defined by the employer relationship in compliance with the Basic Conditions of Employment Act, the Labour Relations Act and Best Practice requirements.

- The employee acknowledges that the collection of their PI is both necessary and it is a legal obligation, that the employer is required to perform in terms of the organisations legal functions and obligations in carrying out the business requirements. The employee therefor unconditionally agrees:

    - That they have been notified of the purpose and/or reason for the collection and processing of their PI as it is a legal requirement that in order for the employer to perform it's functions as an organisation.
    - That they consent and authorise the employer to collect and process the employee's PI in order to facilitate the continued employment of the employee,
    - The employee further consents to the employer's collection and processing of their PI with regards to any Interception and/or communications policies that govern the Organisation's electronic communications.

- To absolve the employer from any liability in terms of PoPIA, for the failure of the employer to obtain the aforesaid consent or to notify the employee of the reason for the processing of any of the employee's PI.
- For the employer to disclose the employee's PI, to any 3rd party, in the instances where the employer has a legal and/or contractual duty to disclose it.
- The employee also agrees to the disclosure of their PI for any reason that the employer may have that is a legitimate requirement for the employer to perform its business on a day to day basis.
- The employee authorises the employer their PI outside of the Republic of South Africa for any legitimate business purpose of the employer with within the international community and the employer undertakes to do this only where necessary and it will comply with the legislative stipulations in this regard.
- The employee will from time to time in the course of the performance of their duties, gain access to the personal information of certain clients, suppliers and/or other employees. The employee will treat this personal information with respect to the privacy of the client/supplier and/or other employees and as a confidential business asset.
- To the extent that the employee is exposed to the PI of clients/suppliers or other employees the employee agrees to be bound by the appropriate and legal binding of confidentiality and non-usage obligations.
- Employees may not directly or indirectly, utilise, disclose or make public in any way to any person or 3rd party, both within the organisation or externally, any PI unless that information is already publically known or that the disclosure of such information is necessary for the employee to perform their duties on behalf of the employer.

ANNEXURE E: SLA CONFIDENTIALITY CLAUSE

SLA CONFIDENTIALITY CLAUSE

- " Personal Information" (PI) refers to the race, gender, sex, marital status, national or ethnic origin, colour, sexual orientation, age, physical or mental health, disability, physical appearance, religion, conscience belief and/or culture, language, and birth of a person. It also pertains to any information relating to the medical financial, criminal or employment history of the person; any identifying number and/or symbol, e-mail address, physical address, telephone and/or cell number, location information, online identifier or any other particular and/or specific assignment to the person; the biometric information of the employee; the personal opinions, views or preferences of the employee; correspondence sent by the employee that is specifically or implicitly of a private and/or confidential nature or further correspondence that would in any way reveal the contents of the original correspondence; the views or opinions of another individual about the person, whether or not the information is recorded electronically or documented or any other way in which it is communicated.
- 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 they may come into contact with, or have access to PI and other information that may be noted as and/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. Furthermore, it is agreed by the parties that they have the necessary consent to share or disclose the PI and that the information they have may have value.
- The parties further agree that they will, at all times comply with PoPIA's Regulations as well at the Code of Conduct and that it shall only collect, use and process PI in a lawful manner and only to the extent that it is required to execute the services and/or provide the goods and/or perform their business and legal obligations in terms of this agreement.
- Both parties agree that they shall put into place, and at all times maintain the appropriate physical, technological and contractual measures to ensure that they both protect the confidentiality of the PI and/or their employees, and/or its contractors and/or any other authorised individuals that they come into contact with.
- Unless it is a legal requirement, the parties also agree that they shall not disclose any PI to any 3rd party without the prior written consent of the other party and will also not transfer an 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 may be withdrawn and/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 example, in the instances where there is a security breach the Information Officer must inform and advise the governing body of their obligations in respect of PoPIA.
- Privacy regulations must be, not only analysed on a regular basis but also aligned with the organisation's personal information processing procedures. This must include reviewing all of the organisation's information protection procedures and related policies.
- Ensure that PoPIA Audits are scheduled on a regular, irregular basis, but at least annually.
- Ensuring that the organisation makes it simple for data subjects, who want to update their personal information or submit PoPIA related complaints to the organisation, to do so. For instance, maintaining a "contact us" facility on the organisation's website.