



**YURI ARCURS PRODUCTIONS (PTY) LTD**  
**Reg. No. 2010/021359/07**

**Protection of Personal Information Act "POPI"**

**Policies**

**Last updated: 28 November 2022**

## 1. INTRODUCTION:

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

The POPI Act 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 organization 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, being able to conduct her 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 the POPI Act's provisions.

The Company is an organisation that always strives to comply with all South African law and recognises that a person's (including employees, customers, and suppliers) Constitutional right to privacy is of the utmost importance, therefore the protection of personal information is vital for sustainability and growth of the business.

## 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:

- 2.1.1 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 person;
- 2.1.2 Information relating to the education or medical, financial, criminal or employment history of the person;
- 2.1.3 Any identifying number, symbol, email address, physical address, telephone number, location information, online identifier, or other particular assignment to the person;
- 2.1.4 Biometric information of the person;
- 2.1.5 The personal opinions, views, or preferences of the person;
  
- 2.1.6 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;

- 2.1.7 The views or opinions of another individual about the person;
  - 2.1.8 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 organization 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 organization is the responsible party.
- 2.4 **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 organization 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 organization's compliance with the POPI Act. Where no information officer is appointed, the head of the organization will be responsible for fulfilling the information officer's duties. Once appointed, the information officer must be registered with the South African Information Regulator established under the POPI Act prior to performing his or her duties. Deputy Information Officers can also be appointed to assist the Information Officer.
- 2.6 **Processing:** the act of processing information includes any activity or any set of operations, whether by automatic means, concerning personal information and includes:
- 2.6.1 The collection, receipt, recording, organization, collation, storage, updating or modification, retrieval, alteration, consultation, or use;
  - 2.6.2 Dissemination by means of transmission, distribution or making available in any other form; or
  - 2.6.3 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:
- 2.7.1 Writing on any material;
  - 2.7.2 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;
  - 2.7.3 Label, marking or other writing which identifies or describes anything of which it forms part, or to which it is attached by any means;
  - 2.7.4 Book, map, plan, graph, or drawing;

- 2.7.5 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.
- 2.8 **Filing System:** means any structured set of personal information, whether centralized, decentralized 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 the responsible party and that uniquely identifies that data subject in relation to that responsible party.
- 2.10 **De-Identify:** 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-Identity:** means any voluntary, specific, and informed expression of will in terms of which permission is given for the processing of personal information.
- 2.12 **Direct Marketing:** means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of:
- 2.12.1 Promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or
- 2.12.2 Requesting the data subject to make a donation of any kind for any reason.
- 2.13 **Biometrics:** means a technique of personal identification that is based on physical, physiological, or behavioural characterization including blood typing, fingerprinting, DNA analysis, retinal scanning, and voice recognition.
- 2.14 In this Code, unless expressly stated otherwise or where the context indicates otherwise, words in the singular shall also mean the plural and other way round, words in the masculine also mean the feminine and the neuter, and words referring to a natural person shall include a reference to a body corporate and the other way around.
- 2.15 The clause headings in this agreement have been inserted for convenience only and will not be taken into consideration in its interpretation.
- 2.16 The contra proferentem rule shall not apply, which shall mean that this agreement and its provisions shall not be adversely interpreted as against the party that drafted such Agreement.
- 2.17 The iusdem generis rule shall not be applicable, which means that when the words “including” followed by specific examples are utilised, such examples shall not be interpreted nor construed as to limit the ambit of the relevant clause of this Agreement.
- 2.18 The words “will”, “shall, and “must” utilised in a set of circumstances that imposes any obligation or restriction on any Party shall have an identical meaning.

### 3. POLICY PURPOSE:

- 3.1 The purpose of this policy is to incorporate the requirements of the Protection of Personal Information Act No. 4 of 2013 (hereafter called the Act) into the everyday operations of the Company and to ensure that these requirements are documented and implemented in the Company to ensure full compliance and adherence to the Act.
- 3.2 Furthermore, this policy tries to protect the organization from the compliance risks associated with the POPI Act which includes:
  - 3.2.1 Breaches of confidentiality. For instance, the organization could suffer loss in revenue where it is found that the personal information of data subjects has been shared or disclosed inappropriately.
  - 3.2.2 Failing to offer choice. For instance, all data subjects should be free to choose how and for what purpose the organization uses information relating to them.
  - 3.2.3 Reputational damage. For instance, the organization could suffer a decline in shareholder value following an adverse event such as a computer hacker deleting the personal information held by an organization.
- 3.3 This policy demonstrates the organization's commitment to protecting the privacy rights of data subjects in the following manner:
  - 3.3.1 Through stating desired behaviour and directing compliance with the provisions of the POPI Act and best practice.
  - 3.3.2 By cultivating an organizational culture that recognizes privacy as a valuable human right.
  - 3.3.3 By developing and implementing internal controls for the purpose of managing the compliance risk associated with the protection of personal information.
  - 3.3.4 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 organization.
  - 3.3.5 By assigning specific duties and responsibilities to control owners, including the appointment of an Information Officer and where necessary, Deputy Information officers, to protect the interests of the organization and data subjects.

#### **4. POLICY APPLICATION**

- 4.1 This policy and its guiding principles apply to:
  - 4.1.1 The Close Corporation's governing body;
  - 4.1.2 managers, supervisors
  - 4.1.3 All branches, business units and divisions of the organization;

- 4.1.4 All employees, i.e., to all staff employed on a casual, contractual, or permanent basis and volunteers;
- 4.1.5 All contractors, suppliers and other persons acting on behalf of the organization.
- 4.2 The policy's guiding principles find application in all situations and must be read in conjunction with the POPI Act, as well as any other applicable documentation (PAIA Manual).
- 4.3** The legal duty to comply with the POPI Act is activated in any situation where there is: a **processing of personal information** entered into a **record** by or for a **responsible party** who is **domiciled in South Africa**.
- 4.4** The POPI Act 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 the personal information has been de-identified.

## 5. Objectives

The CC and its employees shall adhere to this policy in the handling of all personal information received from, but not limited to natural persons, employees, clients, suppliers, agents, representatives, and business partners to ensure compliance with this Act, applicable regulations and other rules relating to the protection of personal information.

The objectives of this policy are:

- Emphasise the company's commitment to ethics and the rule of law.
- To establish a set of uniform rules and regulations which are of a high ethical and legal standard.
- To create a framework, without uncertainty, within which the employees can operate in accordance with the Act.
- To create a structure which allows the prevention and/or detection of wrongdoing.
- To provide clear processes and procedures without ambiguity.
- To protect the interests of both the company and the data subject.

- To balance the right of privacy against other rights, particularly the right of access to information.
- The implementation of corrective action where the Company and/or its employee's actions are unacceptable or do not meet the required standards with regards to the Act.

## **6. Key principles**

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

- To give effect to the Constitutional right to privacy, by safeguarding personal information when processed by the Company, subject to justifiable limitations;
- To regulate the manner in which personal information may be processed, by establishing conditions, in agreement with international standards, that prescribe the minimum requirements for the lawful processing of personal information;
- To be transparent in its standard operating procedures that govern the processing of personal information;
- To comply with the applicable legal and regulatory requirements regarding the processing of personal information;
- To collect personal information through lawful and fair means and to process personal information in a manner compatible with the purpose for which it was collected;
- Where required by law and according to local requirements. To inform data subjects when personal information is collected about them;
- Where required by law, regulations, or guidelines, to obtain a data subject's consent prior to processing his/her/its personal information;
- To strive to keep personal information accurate, complete, up-to-date, and reliable for its intended use;
- To strive to develop reasonable security safeguards against risk, losses, unauthorized access, destruction, use, modification, or disclosure of personal information;
- To strive to provide data subjects with the opportunity to access the personal information relating to them and, where applicable, to comply with requests to correct, amend or rectify the personal information where incomplete, inaccurate, or not compliant with the standard operating procedures;

- To only share personal information, such as permitting access, transmission, or publication, with third parties (either within or outside the Company), only if reasonable assurance can be provided that the recipient of such information will apply suitable privacy and security protection to the personal information;

## **7. Procurement of Personal Information**

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

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

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

**7.3** Steps will be taken to ensure that the data subject is aware of the purpose of the collection of the information.

**7.4** The Company will take reasonably practicable steps to ensure that the personal information is complete, accurate, not missing and updated where necessary, having regard to the purpose for which the personal information is collected and further processed.



7.5 Where personal information is collected from a data subject, the Company will take reasonably practicable steps to ensure that the data subject is aware of:

7.5.1 The information being collected and where the information is not collected from the data subject, the source from which it is collected;

7.5.2 The name and address of the Company;

7.5.3 The purpose for which the information is being collected;

7.5.4 Whether or not the supply of the information by the data subject is voluntary or mandatory;

7.5.5 The consequences of failure to provide the information;

7.5.6 Any particular law authorising or requiring the collection of the information;

7.5.7 The fact that, where applicable, the Company intends to transfer the information to a third country or international organisation and the level of protection offered to the information by that third country or international organisations;

7.5.8 Any further information such as the:

7.5.8.1 Recipient or category of recipients of the information;

7.5.8.2 Nature or category of the information;

7.5.8.3 Existence of the right of access to and the right to rectify the information collected;

7.5.8.4 Existence of the right to object to the processing of personal information;

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

7.6 The steps referred to in clause 7.5 must be taken:

7.6.1 If the information is collected directly from the data subject, prior to the information being collected, unless the data subject is already aware of the information as referred to in clause 7.5;

7.6.2 In any other case, before the information is collected or as soon as reasonably practicable after it has been collected.

7.7 It will not be necessary for the Company to comply with clause 7.5 if:

- 7.7.1 The data subject or a competent person if the data subject is a child has provided consent for the non-compliance;
- 7.7.2 Non-compliance would not prejudice the legitimate interests of the data subject;
- 7.7.3 Non-compliance is necessary:
  - 7.7.3.1 To avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution, and punishment of offences;
  - 7.7.3.2 To comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue;
  - 7.7.3.3 For the conduct of proceedings in any court or tribunal that have commenced or are reasonable contemplated; or
  - 7.7.3.4 In the interest of national security.
- 7.7.4 Compliance would prejudice a lawful purpose of the collection;
- 7.7.5 Compliance is not reasonably practicable in the circumstances of the particular case; or
- 7.7.6 The information will:
  - 7.7.6.1 Not be used in a form in which the data subject may be identified; or
  - 7.7.6.2 Be used for historical, statistical or research purposes.

## **8. Processing of Personal Information**

- 8.1** Personal Information will only be processed lawfully and in a reasonable manner that does not infringe the privacy of the data subject.
- 8.2** Personal Information may only be processed if:
  - 8.2.1** given the purpose for which it was processed, it is adequate, relevant, and not excessive;
  - 8.2.2** the data subject or a competent person where the data subject is a child consents to the processing;
  - 8.2.3** processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party;
  - 8.2.4** processing complies with an obligation imposed by law on the Company;

- 8.2.5** processing protects a legitimate interest of the data subject; or
- 8.2.6** processing is necessary for pursuing the legitimate interest of the Company or of a third party to whom the information is supplied.

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

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

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

## **9. Further Processing of Personal Information**

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

**9.2** To assess whether further processing is compatible with the purpose of collection, the Company will take account of:

- 9.2.1** The relationship between the purpose of the intended further processing and the purpose for which the information was collected;
- 9.2.2** The nature of the information concerned;
- 9.2.3** The consequences of the intended further processing for the data subject;
- 9.2.4** The manner in which the information has been collected; and
- 9.2.5** Any contractual rights and obligations between the parties.

**9.3** The further processing of personal information will not be incompatible with the purpose of collection if:

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

**9.3.1** Further processing is necessary:

- a) To avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution, and punishment of offences;
- b) To comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue;
- c) For the conduct of proceedings in any court or tribunal that have commenced or are reasonable contemplated; or

**9.3.2** The further processing of the information is necessary to prevent or mitigate a serious and imminent threat to:

- a) Public health or public safety; or
- b) The life or health of a data subject or other individual(s);

**9.3.3** The information is used for historical, statistical or research purposes and The Company ensures that the processing is carried out solely for such purposes and will not be published in an identifiable form.

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

**10.1** Records of personal information must not be retained any longer than necessary for achieving the purpose for which the information was collected or subsequently processed, unless:

**10.1.1** The retention of a record is required or authorized by law;

**10.1.2** The Company reasonable requires a record for lawful purposes related to its functions or activities;

**10.1.3** Retention of a record is required by a contact between the parties thereto; or

**10.1.4** The data subject or a competent person where the data subject is a child has consented to the retention of a record.

**10.2** Information collected or processed initially for the purposed of historical, statistical or research value, may be retained for a period longer than contemplated in clause 10.1, providing the Company has appropriate measures in place to safeguard these records against uses other than what it was intended for initially.

**10.3** The Company will destroy or delete a record of personal information or de-identify it as soon as reasonably practicably after The Company is no longer authorized to retain a record.

**10.4** The de-identifying or deletion of a record of personal information must be done in a manner that prevents its reconstruction in an intelligible/understandable form.

**10.5** In the event that The Company uses a record of personal information of a data subject to make a decision about the data subject, it must:

**10.5.1** Retain the record for such period as may be required or prescribed by law or a code of conduct; or

**10.5.2** If there is no law or code of conduct prescribing a retention period, retain the record for a period which will afford the data subject a reasonable opportunity, taking all considerations relating to the use of the personal information into account, to request access to the record.

**10.6** The Company will restrict the processing of personal information if:

**10.6.1** Its accuracy is contested by the data subject, for a period enabling The Company to verify the accuracy of the information;

**10.6.2** The Company no longer needs the personal information for achieving the purpose for which it was collected or subsequently processed, but it has to be maintained for purposes of proof;

**10.6.3** The processing is unlawful, and the data subject opposed its destruction or deletion and request the restriction of its use instead; or

**10.6.4** The data subject requests to transit the personal data into another automated processing system.

**10.7** Personal information that has been restricted may only be processed for purposes of proof, or with the data subject's consent, or with the consent of a competent person where the data subject is a child, or for the protection of the rights of another natural or legal person or if such processing is in the public interest.

**10.8** Where the information is restricted, The Company will inform the data subject before lifting the restriction.

## **11. Security Safeguards**

**11.1** The Company will secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable, technical, and organisational measures to prevent:

**11.1.1** Loss of, damage to or unauthorized destruction of personal information; and

**11.1.2** Unlawful access to or processing of personal information.

**11.2** The Company will take reasonable measures to:

**11.2.1** Identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;

- 11.2.2** Establish and maintain appropriate safeguards against the risks identified;
  - 11.2.3** Regularly verify that the safeguards are effectively implemented; and
  - 11.2.4** Ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.
- 11.3** The Company will have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations.
- 11.4** The Company will, in terms of a written contract between The Company and the operator, ensure that the operator which processes personal information for The Company, establishes and maintain security measures.
- 11.5** The operator will inform The Company immediately where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorized person.

## **12. Security Compromises**

- 12.1** Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorized person, The Company will notify:
- 12.1.1** The Information Regulator; and
  - 12.1.2** The data subject unless the identity of such data subject cannot be established.
- 12.2** The notification of a breach will be made as soon as reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of The Company's information system.
- 12.3** The Company will only delay notification of the data subject if a public body responsible for the prevention, detection or investigation of offences or the Regulator determines that notification will impede a criminal investigation by the public body concerned.
- 12.4** The notification to a data subject will be in writing and communicated to the data subject in at least one of the following ways:
- 12.4.1** Posted to the data subject's last known physical or postal address; or
  - 12.4.2** Sent by e-mail to the data subject's last known e-mail address; or
  - 12.4.3** Placed in a prominent position on the website of The Company; or

**12.4.4** Published in the news media.

**12.5** The notification will provide sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise, including:

**12.5.1** A description of the possible consequences of the security compromise;

**12.5.2** A description of the measures that The Company intends to take or has taken to address the security compromise;

**12.5.3** A recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise; and

**12.5.4** If known to The Company, the identity of the unauthorized person who may have accessed or acquired the personal information.

### **13. Rights of the Data Subject**

**13.1** The data subject or competent person where the data subject is a child, may withdraw his, her or its consent to procure and process his, her or its personal information, at any time, providing the lawfulness of the processing of the personal information before such withdrawal or the processing of personal information in terms of clause 9 is not affected.

**13.2** A data subject may object, at any time, to the processing of personal information:

**13.2.1** In terms of clause 9 in writing, on reasonable grounds relating to his/hers or its particular situation, unless legislation provides for such processing; or

**13.2.2** For purposes of direct marketing other than direct marketing by means of unsolicited electronic communications.

**13.3** A data subject, having provided adequate proof of identity, has the right to:

**13.3.1** Request the Company to confirm, free of charge, whether or not the Company holds personal information about the data subject; and

**13.3.2** Request from The Company a record or a description of the personal information about the data subject held by The Company, including information about the identity of all third parties, or categories of third parties, who have, or have had, access to the information:

**13.3.2.1** Within a reasonable time;

**13.3.2.2** At a prescribed fee as determined by the Information Officer;

**13.3.2.3** In a reasonable manner and format; and

**13.3.2.4** In a form that is generally understandable.

**13.4** A data subject may, in the prescribed manner, request The Company to:

**13.4.1** Correct or delete personal information about the data subject in its possession or under its control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or obtained unlawfully; or

**13.4.2** Destroy or delete a record of personal information about the data subject that The Company is no longer authorized to retain.

**13.5** Upon receipt of a request referred to in clause 14.4, The Company will, as soon as reasonably practicable:

**13.5.1** Correct the information;

**13.5.2** Destroy or delete the information;

**13.5.3** Provide the data subject, to his, her or its satisfaction, with credible evidence in support of the information; or

**13.5.4** Where an agreement cannot be reached between The Company and the data subject, and if the data subject so requests, take such steps as are reasonable in the circumstances, to attach to the information in such a manner that it will always be read with the information, an indication that a correction of the information has been requested but not been made.

**13.6** The Company will inform the data subject, who made a request, of the action as a result of the request.

#### **14. Request for Disclosure**

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

#### **15. Monitoring and Enforcement**

Each employee of the Company, who is deemed an Operator, will be responsible for administering and overseeing the implementation of this policy and, as applicable, supporting guidelines, standard operating procedures, notices, consents and appropriate related documents and processes. Managers and responsible employees will be trained according to the functions in legal requirements, policies and guidelines that govern the protection of personal information in The Company. The Company will conduct periodic reviews and audits, where appropriate, to demonstrate compliance with privacy law and its policies, this Act, and any applicable regulations. Employees



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

## **16. Point of Contact**

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

## **17. Standard Operating Procedures**

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

# **PROTECTION OF PERSONAL INFORMATION & BREACH PROTOCOL**

## **1. RIGHTS OF DATA SUBJECTS**

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

### **1.1. The right to access of personal information**

1.1.1. The organization recognizes that a data subject has the right to establish whether the organization holds personal information related to him, her, or it, including the right to request access to that personal information.

### **1.2. 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.

### **1.3. 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 organization will give due consideration to the request and the requirements of POPIA. The organization 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.

#### **1.4. 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.

#### **1.5. 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.

#### **1.6. 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 situation where the organization has reasonable grounds to believe that the personal information of the data subject has been accessed or acquired by an unauthorised person.

### **2. 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:

#### **2.1. Accountability**

Failing to comply with the POPI Act 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 are 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.

#### **2.2. Processing Limitation**

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

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

### **2.3. Purpose Specification**

All 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.

### **2.4. 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.

### **2.5. 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 (for example, the beneficiary details of a life insurance policy are of the utmost importance), the greater the effort the organisation will put into ensuring its accuracy. Where personal information is collected or received from third parties, the 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.

### **2.6. 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" 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;
- Request access to related personal information;
- Request the organisation to update or correct related personal information; or
- Make a complaint concerning the processing of personal information.

## **2.7. Security Safeguards**

- 2.7.1. 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 to minimise the risk of loss, unauthorised access, disclosure, interference, modification, or destruction. Security measures also need to be applied in a context-sensitive manner. For example, the more sensitive the personal information, such as medical information or credit card details, the greater the security required.
- 2.7.2. 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.
- 2.7.3. All new employees will be required to sign employment contracts containing contractual terms for the use and storage of employee information. Confidentiality clauses will also be included to reduce the risk of unauthorised disclosures of personal information for which the organisation is responsible. All existing employees will, after the required consultation process has been followed, be required to sign an addendum to their employment containing the relevant consent and confidentiality clauses.
- 2.7.4. 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.

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

## **3. INFORMATION OFFICER**

- 3.1. 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.
- 3.2. 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.
- 3.3. 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.

## **4. SPECIFIC DUTIES AND RESPONSIBILITIES**

### **4.1. Governing Body/Board of Directors**

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. 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:

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

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

4.1.2.1. are appropriately trained and supervised to do so;

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

4.1.2.3. are aware that a wilful or negligent breach of this policy's processes and procedures may lead to disciplinary action being taken against them.

4.1.3. 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.

4.1.4. 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.

### **4.2. Information officer**

The organisation's Information Officer is responsible for:

4.2.1. Taking steps to ensure the organisation's reasonable compliance with the provision of POPIA.

4.2.2. 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.

4.2.3. 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.

4.2.4. Ensuring that POPI Audits are scheduled and conducted on a regular basis.

- 4.2.5. 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.
- 4.2.6. Approving any contracts entered 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.
- 4.2.7. Encouraging compliance with the conditions required for the lawful processing of personal information.
- 4.2.8. 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.
- 4.2.9. Organising and overseeing the awareness training of employees and other individuals involved in the processing of personal information on behalf of the organisation.
- 4.2.10. Addressing employees’ POPIA related questions.
- 4.2.11. Addressing all POPIA related requests and complaints made by the organisation’s data subjects.
- 4.2.12. 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 appropriate, regarding any other matter.

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

#### **4.3. IT Manager / IT Support**

The organisation’s IT Manager or IT Support is responsible for:

- 4.3.1. Ensuring that the organisation’s IT infrastructure, filing systems and any other devices used for processing personal information meet acceptable security standards.
- 4.3.2. Ensuring that all electronically held personal information is kept only on designated drives and servers and uploaded only to approved cloud computing services.
- 4.3.3. Ensuring that servers containing personal information are sited in a secure location, away from the general office space.
- 4.3.4. Ensuring that all electronically stored personal information is backed-up and tested on a regular basis.

- 4.3.5. Ensuring that all back-ups containing personal information are protected from unauthorised access, accidental deletion, and malicious shacking attempts.
- 4.3.6. Ensuring that personal information being transferred electronically is encrypted.
- 4.3.7. Ensuring that all servers and computers containing personal information are protected by a firewall and the latest security software.
- 4.3.8. Performing regular IT audits to ensure that the security of the organisation's hardware and software systems are functioning properly.
- 4.3.9. Performing regular IT audits to verify whether electronically stored personal information has been accessed or acquired by any unauthorised persons.
- 4.3.10. 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 instance, cloud computing services.

#### **4.4. Marketing & Communications Manager / Team**

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

- 4.4.1. 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.
- 4.4.2. Addressing any personal information protection queries from journalists or media outlets such as newspapers.
- 4.4.3. Where necessary, working with persons acting on behalf of the organisation to ensure that any outsourced marketing initiatives comply with POPIA.

#### **4.5. Employees and other persons acting on behalf of the Organisation**

- 4.5.1. 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.
- 4.5.2. 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.
- 4.5.3. 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.

- 4.5.4. 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 any aspect related to the protection of a data subject's personal information.
- 4.5.5. Employees and other persons acting on behalf of the organisation will only process personal information where:
- 4.5.5.1. The data subject, or a competent person where the data subject is a child, consents to the processing; or
  - 4.5.5.2. 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
  - 4.5.5.3. The processing complies with an obligation imposed by law on the responsible party; or
  - 4.5.5.4. The processing protects a legitimate interest of the data subject; or
  - 4.5.5.5. The processing is necessary for pursuing the legitimate interests of the organisation or of a third party to whom the information is supplied.
- 4.5.6. Furthermore, personal information will only be processed where the data subject:
- 4.5.6.1. Clearly understands why and for what purpose his, her or its personal information is being collected; and
  - 4.5.6.2. Has granted the organisation with explicit written or verbally recorded consent to process his, her or its personal information.
- 4.5.7. 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.
- 4.5.8. 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.
- 4.5.9. 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.
- 4.5.10. Consent to process a data subject's personal information will be obtained directly from the data subject, except where:
- 4.5.10.1. the personal information has been made public;
  - 4.5.10.2. where valid consent has been given to a third party; or
  - 4.5.10.3. the information is necessary for effective law enforcement.
- 4.5.11. Employees and other persons acting on behalf of the organisation will under no circumstances:



- 4.5.11.1. 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.
  - 4.5.11.2. 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.
  - 4.5.11.3. 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.
  - 4.5.11.4. Transfer personal information outside of South Africa without the express permission from the Information Officer.
- 4.5.12. Employees and other persons acting on behalf of the organisation are responsible for:
- 4.5.12.1. Keeping all personal information that they come into contact with secure, by taking sensible precautions and following the guidelines outlined within this policy.
  - 4.5.12.2. Ensuring that personal information is held in as few places as is necessary. No unnecessary additional records, filing systems and data sets should therefore be created.
  - 4.5.12.3. 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.
  - 4.5.12.4. 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 regularly and may not be shared with unauthorised persons.
  - 4.5.12.5. Ensuring that their computer screens and other devices are switched off or locked when not in use or when away from their desks.
  - 4.5.12.6. 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.
  - 4.5.12.7. Ensuring that where personal information is stored on paper, that such hard copy records are kept in a secure place where unauthorised people cannot access it. For instance, in a locked drawer of a filing cabinet.
  - 4.5.12.8. 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.
  - 4.5.12.9. 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.

- 4.5.12.10. 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 or the Information Officer to delete or dispose of the personal information in the appropriate manner.
- 4.5.12.11. Undergoing POPI Awareness training from time to time.

4.5.13. 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.

## **5. POPI AUDIT**

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

5.2. The purpose of the POPI Audit is to:

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

5.3. 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.

## **6. REQUEST TO ACCESS PERSONAL INFORMATION**

6.1. Data subjects have the right to:

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

6.1.2. Request access to their personal information.

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

6.2. 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".

6.3. 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.

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

## **7. POPI COMPLAINTS PROCEDURE**

7.1. 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 POPI related complaints in accordance with the following procedure:

7.1.1. 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".

7.1.2. 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.

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

7.1.4. 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.

7.1.5. 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.

7.1.6. 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 where after the affected data subjects and the Information Regulator will be informed of this breach.

7.1.7. 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.

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

7.1.8.1. A suggested remedy for the complaint,

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

7.1.8.3. An apology (if applicable) and any disciplinary action that has been taken against any employees involved.

7.1.9. 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.

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

## **8. PERSONAL DATA BREACH PROTOCOL**

8.1. For the purposes of this section, a personal data breach is any attempt at, or occurrence of, unauthorized acquisition, exposure, disclosure, use, modification, or destruction of personal and/or sensitive data as described in this policy. The breach protocol is meant to address security incidents involving any and all personal data held, collected, processed and/or stored by the Organisation, including personal data under the control or responsibility of an affiliated business or third party.

8.2. The Organisation shall ensure that, *inter alia*, all personal data breaches are reported to the Regulator, investigated, and contained within the Organisation or by the Organisation and in terms of this policy.

8.3. The following is an indication of the timelines necessary herein and to be followed by the Organisation and/or its Information Officer when responding to, investigating, and reporting on any personal data breach within the Organisation:

### **8.3.1. Initial response to discovering personal data breach, or potential breach:**

8.3.1.1. Identifying personal data breach or potential breach;

8.3.1.2. Involvement of Information Officer, IT/Server Department and any necessary and/or applicable parties;

- 8.3.1.3. Involvement of compliance department, legal department or similar (if applicable to the Organisation).

#### 8.3.2. Immediate Response (0--1 Business Day):

- 8.3.2.1. Containment
- 8.3.2.2. Opening of Incident Report or POPI Breach report;
- 8.3.2.3. Escalation to the relevant individuals or authoritative body(ies);
- 8.3.2.4. Activation of initial response plan and/or containment plan.

#### 8.3.3. Continuing Response (0-15+ days)

- 8.3.3.1. Analysis and Planning (both in terms of closure of the pending breach and initiation of any plans regarding prospective breaches or the avoidance thereof);
- 8.3.3.2. Investigation;
- 8.3.3.3. Mitigation and Correction;
- 8.3.3.4. Notification;
- 8.3.3.5. Closing of Incident Report or POPI Breach report;
- 8.3.3.6. Final reporting (Information Officer, Regulator and Data Subjects).

- 8.4. Initial Response: the Organisation must take proactive steps to ensure that any personal data breach or potential breach is identified as soon as reasonably possible. Once identified, the Organisation, through its IT department and Information Officer, must bring the personal data breach or potential breach to the attention of the necessary parties who will be responsible for containing the personal data breach or potential breach.
- 8.5. Immediate Response: the Organisation, its IT department and the Information Officer must, when a breach is discovered, conduct containment activities to stop additional information from being lost or disclosed, or to reduce the number of persons to whom personal information may reach. The Organisation may, over its areas of responsibility or collaboratively, take steps to attempt having lost/stolen/inappropriately disclosed information returned or destroyed. For instance, area managers may attempt to contain and control an incident by suspending certain activities or locking and securing areas of record storage; Human Resources may suspend employees as appropriate to prevent compromising behaviour; and the Information IT Department may shut down particular applications or third-party connections, reconfigure firewalls, change computer access codes, or change physical access codes.
- 8.6. If applicable, staff members closest to the incident will determine the extent of the breach or potential breach by identifying all information (and systems) affected and take action to stop the exposure. This may include:
  - 8.6.1. Securing or disconnecting affected systems;
  - 8.6.2. Securing affected records or documentation;
  - 8.6.3. Halting affected business processes;
  - 8.6.4. Pausing any processes that may rely on exposed information or that may have given rise to the incident (as necessary to prevent further use/exposure/etc)

This would most typically occur in instances of electronic system intrusion, exposed physical (e.g., medical) files or records or similar situations.

- 8.7. If an active cyber-insurance policy exists or the need is otherwise determined, the Organisation or its Information Officer may contact contracted third parties (cyber-insurance vendors or affiliates) for breach response services and resources to include forensics, investigation and response consulting, notification, and call center services. Though recommended to occur as soon as possible after discovery, this can occur at any point as more information is obtained or the need is otherwise determined.
- 8.8. All documentation, investigation and initial and/or containment reports must be kept throughout the personal data breach protocol procedure and included in any report from the Information Officer to the Regulator in terms of section 22 of the POPI Act.
- 8.9. As more information is gathered, responsible staff will assess each personal data breach or potential breach to determine appropriate handling. This may involve the development and use of internal procedures by individual departments. For instance, while a minor and low risk incident may be assigned to and investigated by competent technicians within a department, the department may require that technician to escalate to management any incident that may damage the Organisation. The manager, in turn, may escalate the incident to the director, VP, or other level (subject to the Organisation's internal structure and/or organogram).
- 8.10. This may also involve activating alternate plans – for instance, Data Recovery Plans and/or any applicable alternative.
- 8.11. Additionally, responsible departments will assess each personal data breach to determine which parties should be included in communications and/or the further reporting of the personal data breach incident. For instance, the Organisation or Information Officer may grant certain access and permissions pertaining to cases to include area managers, directors, and vice-presidents unless circumstances exist that would preclude sharing information – for instance, if a conflict of interest exists; if sharing the information could compromise an investigation; or if the responsible manager (or a friend or family member of the responsible manager) is involved as an affected party, as a subject, or in other ways.
- 8.12. Continued response and reporting to the Regulator: all efforts, including but not limited to the initial reporting; the containment and any containment plans; any further planning and proposed corrections; and/or record of any correspondence or notice sent to any of the Organisation's affected data subjects must be kept and form a material part of the final incident report submitted to the Regulator in terms of section 22 of the POPI Act.
- 8.13. After containment of the personal data breach and implementation of any necessary containment plan; interim plan or relief; correction plan; data recovery plan; and/or similar plan implemented in response to the personal data breach, the Organisation's Information Officer must prepare a written report to submit to the Regulator.
- 8.14. The aforementioned written report must contain all necessary and material information pertaining to the personal data breach, including but not limited, any supporting documentation, investigation outcomes and/or improvement plans. The report must indicate whether the breach was low, moderate, or high risk and the extent of the personal data

breach, including but not limited to any actual damages suffered; any damage or injury to affected data subjects; and any potential or further threat created by the personal data breach.

8.15. The Information Officer must further notify all affected data subjects of the personal data breach as soon as reasonably possible after discovery of the personal data breach, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the breach and to restore the integrity of the Organisation's information system. The notification must be done in writing and communicated to the data subject in one of the following ways:

- 8.15.1. Mailed to the data subject's last known physical or postal address;
- 8.15.2. Sent by email to the data subject's last known email address;
- 8.15.3. Placed in a prominent position on the website of the Organisation;
- 8.15.4. Published in the news or media; or
- 8.15.5. As may be directed by the Regulator.

8.16. The notification must provide the affected data subjects with sufficient information to allow the data subject to take protective measures against the personal data breach, including –

- 8.16.1. A description of the possible consequences of the breach;
- 8.16.2. A description of the measures that the Organisation intends to take or has taken to address the personal data breach and/or security compromise;
- 8.16.3. A recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the personal data breach; and
- 8.16.4. The identity of the unauthorised person or entity who may have accessed or acquired personal information, if known to the Organisation.

8.17. The Regulator may direct an Organisation to publicise, in any manner specified, the fact of any personal data breach or compromise to the integrity of personal information, if the Regulator has reasonable grounds to believe that such publicity would protect a data subject who may be affected by the breach.

## **9. DISCIPLINARY ACTION**

9.1. 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.

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

9.3. 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.

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

9.4.1. A recommendation to commence with disciplinary action.

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

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