GERATEC

GERALEARN GERASERVE GERACONSULT

POPIA NOTICE

POPIA POLICY

POPIA POLICY (DATA PROTECTION POLICY)

POPIA POLICY (DATA PROTECTION POLICY)

Statement from the Board of Directors

The Organization, **Geracare (Pty) Ltd**, has a proud tradition of conducting business in accordance with the highest ethical standards and in full compliance with all applicable laws.

The Data Protection Policy was developed at the direction of the Organization's Board of Directors to provide clear guidance to all directors, employees and those who process personal information on behalf of the Organization to ensure a lawful, transparent and consistent approach to the processing of personal information.

The Organization's Board of Directors is fully committed to conduct business with the highest level of integrity and we expect your strict adherence to this Data Protection Policy and the law.

The Organization has adopted a zero-tolerance stance in relation to any non-compliance with its policies, including this Policy.

Any violation of this Policy will result in swift corrective action, including possible termination of employment, and criminal and civil action.

Thank you for your commitment to comply unequivocally with the highest standards of integrity and business ethics.

Document Control			
Document type	Information Governance Policy		
Document owner	Information Officer		
Division			
Lead contact	Information Officer		
Document status	Approved		
Version	v1.0		
Approved by		**Date**	
Date of publication		**Next review date**	
Date of original publication		**Revision frequency**	2 years
Superseded documents	N/A		
Related documents			

Information Officer Approval: Victor Southwell **Signed:** 

CONTENTS

Information Officer Approval: Victor Southwell **Signed:**

Information Officer Approval: Victor Southwell **Signed:**

BACKGROUND TO PERSONAL INFORMATION PROTECTION

PERSONAL INFORMATION PROCESSING LAWS

In South Africa (SA), legislators have defined under a law known as the Protection of Personal Information Act, 4 of 2013 (POPIA), certain data processing principles and related standards, for the protection of personal information, which law applies to both natural and legal persons, including the requirement that such personal information may only be transferred to other countries if the local law applicable at the place of destination provides for similar levels or standards of data protection as that afforded by POPIA.

AREAS WHERE THE ORGANIZATION PROCESSES PERSONAL INFORMATION

The Organization provides the highest quality and innovative contract services to older persons in long term residential facilities. In addition, we provide food and beverage services and our Care and Support Teams provide a comprehensive range of clinical care services, including companionship, assistance with activities of daily life and specialised clinical nursing care when needed.

Inherent in the provision of these goods and services, the Organization continually has access to and needs to process personal information and information relating to individuals and legal entities.

This Policy sets out how the Organization processes personal information in order to meet the data protection standards of the Organization and in order to comply with the legal standards as laid down under POPIA.

PURPOSE OF POLICY

The Organization considers the safeguarding of data protection rights as part of its social responsibility.

This Data Protection Policy seeks to ensure that the Organization:

- complies with national and international legal standards and best practices for the receipt, importing, processing, handling, storing, sharing and disposal of personal information belonging to individuals and legal entities ("data subjects"), which data subjects include without detracting from the generality, employees, service providers, clients, and third parties;
- protects the privacy rights of all data subjects who it engages with;
- is transparent in relation to the processing of personal information, especially in relation to what personal information it collects, the reasons for such collection and how it collects, handles, shares, stores and destroys such personal information;
- is aware of the risks it faces in relation to personal information including data breaches, unlawful access to personal information, loss of data or poor governance of data, thereby allowing it to implement the required data protection controls in order to manage these data risks.

Importantly, this Data Protection Policy establishes uniform and suitable data protection procedures and standards within the Organization for the processing of personal information

In line with the above this Policy sets out:

- the Organization's responsibilities under POPIA and how it will comply with POPIA;
- how the Organization processes personal information which is owned, applies to and / or relates to identifiable or identified individuals and legal entities, including employees, service providers, and other third parties, known as data subjects;
- the instruction for directors, employees and other Organization representatives when handling personal information.

Information Officer Approval: Victor Southwell **Signed:**

GLOSSARY
The term “data privacy” is used in this policy as an umbrella term to encompass concepts of autonomy, privacy, data protection, security and responsible data management. The term “personal information” is used in this policy to describe any information relating an identified or identifiable natural person and any identified or identifiable legal entity (“data subject”), consistent with the provisions of the South African Data Privacy law, known as the Protection of Personal Information Act, 4 of 2013 (“POPIA”). Other references made throughout this Policy can be found under **Schedule 1.**
SCOPE
The Policy applies to all directors, employees and other Organization representatives who are carrying out work on behalf of the Organization. The rules and standards set out in this Policy applies to all personal information processed by the Organization in an automated or non-automated manner, and regardless of how stored or recorded, i.e., stored electronically, digitally, on paper, or on other materials, or through other methods.

Information Officer Approval: Victor Southwell **Signed:**

1. INTRODUCTION

1.1 The protection of individuals and legal entities' personal information is a fundamental constitutional and human right.

1.2 In accordance with POPIA, the Organization has a duty to ensure that all person's personal information is processed in a legitimate, lawful and responsible manner.

1.3 Failure to comply with POPIA, may have severe consequences for the Organization, including criminal sanctions, civil claims and damages and potential administrative fines of up to R10 000 000 in South Africa.

2. PURPOSE OF THIS POLICY

2.1 This Policy sets out how the Organization will process the personal information which is owned, applies to and / or relates to identifiable or identified individuals and legal entities, including employees, service providers, and other third parties, known as data subjects.

2.2 This Policy applies to all personal information that the Organization processes regardless of the format or media on which the data is stored or who it relates to.

2.3 A glossary of the terms used throughout the Policy can be found in Schedule 1.

3. SCOPE OF THIS POLICY

3.1 This Policy applies to all directors, employees and other Organization representatives who are carrying out work on behalf of the Organization.

3.2 All directors, employees and other representatives or persons who process personal information on behalf of the Organization are without exception expected to comply with the Organization's legal obligations in so far as they relate to the handling and processing of personal information, which has to be done in order to protect the Organization from the risk of non-compliance, and the consequences of such non-compliance, including loss of data, investigations, administrative penalties, criminal charges and fines, civil claims and damages, as well as reputational risk.

3.3 All directors, employees and other representatives or persons who process personal information on behalf of the Organization must read, understand and comply with this Policy when processing personal information in the course of performing their tasks and must

Information Officer Approval: Victor Southwell **Signed:** 

observe and comply with all personal information controls, practices, protocols and training to ensure such compliance.

4. COMPLIANCE WITH THIS POLICY AND THE RELATED POLICIES AND PROCEDURES SET OUT IN THE SCHEDULES IS MANDATORY.

5. ANY BREACH OF THIS POLICY AND THE RELATED POLICIES AND PROCEDURES MAY RESULT IN DISCIPLINARY ACTION AND POSSIBLE CRIMINAL AND / OR CIVIL ACTION.

6. DATA PROTECTION PRINCIPLES

6.1 POPIA is based on a set of core principles that the Organization must observe and comply with at all times from the moment that personal information is collected until the moment that personal information is archived, deleted or destroyed. These principles are detailed below.

6.1.1 Accountability

6.1.1.1 The Organization is responsible for and must be able to demonstrate compliance with the data protection principles and the Organization's other obligations under POPIA. This is known as the 'accountability principle'.

6.1.2 Lawfulness, fairness and transparency

6.1.2.1 The Organization must only process personal information in a lawful, fair and in a transparent manner.

6.1.3 Purpose limitation

6.1.3.1 The Organization must only collect and process personal information for a specified, explicit and legitimate purpose.

6.1.4 Data minimisation

6.1.4.1 The Organization must ensure that personal information which is processed by it is adequate, relevant and limited to what is necessary in relation to the purposes for which it is to be processed.

Information Officer Approval: Victor Southwell **Signed:** 

6.1.5 Accuracy

6.1.5.1 The Organization must ensure that personal information which is processed by it is accurate and where necessary kept up to date.

6.1.6 Storage limitation

6.1.6.1 The Organization must ensure that personal information which is processed by it is not kept for longer than is necessary for the purposes for which the data is processed.

6.1.7 Security, integrity and confidentiality

6.1.7.1 The Organization must ensure that personal information which is processed by it is done in a manner that ensures its security using appropriate technical and organisational measures to protect the data against unauthorised or unlawful processing and against accidental loss, destruction or damage.

6.1.8 Transfers of personal information outside the Processing territories

6.1.8.1 The Organization must ensure that personal information which is processed by it is not transferred to countries outside of South Africa, which do not have similar data privacy laws in place, unless appropriate safeguards are put in place by the Organization which provide the data subject with the same rights and levels of protection is so far as its personal information is concerned, as provided for under POPIA, in such countries.

6.1.9 Data subject rights and requests

6.1.9.1 The Organization must allow data subjects to exercise their rights in relation to their personal information.

7. PROCESSES IMPLEMENTED BY THE ORGANIZATION IN ORDER TO ENSURE THAT THE DATA PROTECTION PRINCIPLES ARE GIVEN EFFECT TO

7.1 The Organization must ensure that it has adequate resources, systems and processes in place to demonstrate compliance with its data processing obligations including:

7.1.1 appointing a suitably qualified and experienced Information Officer under POPIA and where required deputy information officers and providing them with adequate support and resource;

7.1.2 ensuring that at the time of deciding how the Organization will process personal information, and throughout its processing, implementing appropriate technical and organisational measures that are designed to ensure compliance with the data protection principles;

7.1.3 ensuring that, by default, only personal information that is necessary for each specific purpose are processed both in relation to the nature, extent and volume of such personal information, the period of storage and the accessibility of the personal information;

7.1.4 ensuring that where any intended processing presents a high risk to the rights and freedoms of data subjects, the Organization has carried out an assessment of those risks and is taking steps to mitigate those risks, by undertaking a 'Data Protection Impact Assessment';

7.1.5 integrating data protection into the Organization's internal procedures and documents, by way of privacy policies and processing notices;

7.1.6 regularly training the Organization's directors, employees and those who process personal information on behalf of the Organization on POPIA, this Policy and the Organization's related policies and procedures, and maintaining a record of all such training;

7.1.7 regularly testing the measures implemented by the Organization and conducting periodic reviews to assess the adequacy and effectiveness of this Policy, and the Organization's related personal information policies and procedures, which procedures are more fully described below.

7.2 Lawfulness and consent to process under certain circumstances

7.2.1 In order to collect and process personal information for any specific purpose, the Organization must always have a lawful basis and purpose for doing so.

7.2.2 Consent to process a data subject's personal information will not always be required. The Organization in terms of POPIA will be allowed to lawfully process a data subject's personal information without the data subject's consent under the following circumstances:

7.2.2.1 The processing is necessary **for the conclusion of or for the performance of a contract** to which the data subject is a party (for instance a contract of employment or registration with the Organization as a vendor);

7.2.2.2 The processing is necessary in order for the Organization to **comply with certain legal obligations** (for instance, to comply with the labour laws);

7.2.2.3 The processing is in order to **protect the legitimate or vital interests of the data subject**, or the Organization or of another

Information Officer Approval: Victor Southwell **Signed:** 

person (this will equate to a situation where the processing is necessary to protect the individual's life);

7.2.2.4 The processing is in order to **perform a public duty** or to perform tasks carried out in the public interest or the exercise of official authority.

7.2.3 Where the processing of a data subject's personal information is required for purposes which are not detailed under section 7.2.2 above, then in such circumstances, in order to legitimise and ensure that such processing is lawful, the data subject **has to agree to such processing**, i.e., it has to provide consent to the processing of its personal information. In this regard it's important to note that where the processing is taking place in South Africa, then the consent can be implied – i.e., consent can be done by way of a gesture or simple indication of agreement.

7.2.4 Furthermore, where consent is required from the data subject, then such consent must be freely and genuinely given (there must not be any imbalance in the relationship between the Organization and the data subject and consent must not be a condition for the provision of any product or service).

7.2.5 Where, in terms of POPIA, consent to process a data subjects' personal information is required, such consent may at any time be withdrawn by the data subject. If consent is withdrawn, then the Organization will no longer be allowed to continue processing such personal information from the date of such withdrawal and so it will be important to advise the data subject of the consequences of the withdrawal, i.e., that the Organization will not be able to continue its relationship with the data subject.

7.2.6 Where a third party provides the Organization with another's personal information (for example, CVs housing a job applicant's personal information provided by a recruitment agents or credit bureaux records housing Personal Information about a creditor which is provided by a credit bureaux in relation to a data subject's credit worthiness or where personal information pertaining to service provider's employee is provided by a service provider) the Organization must obtain confirmation that it was collected by the third party in accordance with the data privacy law requirements and that such personal information was lawfully processed, and that the sharing of the personal information with the Organization was clearly explained to the data subject by such third party and where required permission to process including the passing on or the sharing of information was obtained from the owner thereof.

7.2.7 POPIA distinguish between personal information and "special personal information" which is also known as "sensitive personal information". Special data concerns the data subject's race, ethnicity, politics, religion, trade union membership, genetics, biometrics, health, sex life, or sexual orientation.

7.2.8 Under POPIA, in order to process special personal information, being the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or the criminal behaviour of a data subject to the extent that such information relates to the alleged commission by a data subject of any offence; or any proceedings in respect of any offence allegedly committed by a data subject or

Information Officer Approval: Victor Southwell **Signed:**

the disposal of such proceedings, the following has to be shown in relation to such processing:

7.2.8.1 the processing is carried out with the consent of a data subject;

7.2.8.2 the processing is necessary for the establishment, exercise or defence of a right or obligation in law;

7.2.8.3 the processing is necessary to comply with an obligation of international public law;

7.2.8.4 the processing is for historical, statistical or research purposes to the extent that the purpose serves a public interest and the processing is necessary for the purpose concerned; or it appears to be impossible or would involve a disproportionate effort to ask for consent, and sufficient guarantees are provided for to ensure that the processing does not adversely affect the individual privacy of the data subject to a disproportionate extent;

7.2.8.5 the information has deliberately been made public by the data subject;

7.2.8.6 permission has been received from the Information Regulator to process special personal information if such processing is in the public interest and appropriate safeguards have been put in place to protect the personal information of the data subject;

7.2.8.7 where the processing concerns religious or philosophical beliefs, and such processing has been done and is necessary to protect the spiritual welfare of the data subjects, unless they have indicated that they object to the processing, and provided that such information is not supplied to third parties without the consent of the data subject;

7.2.8.8 where the processing concerns race or ethnic origin, and such processing is carried out to identify data subjects and only when this is essential for that purpose; and to comply with laws and other measures designed to protect or advance persons, or categories of persons, disadvantaged by unfair discrimination;

7.2.8.9 where the processing concerns trade union membership, and such processing is carried out by the trade union because it is necessary to achieve the aims of the trade union or trade union federation and provided that such information is not supplied to third parties without the consent of the data subject;

7.2.8.10 where the processing concerns one's health or sex life, and such processing is carried out by

a) medical professionals, healthcare institutions or facilities or social services, if such processing is necessary for the proper treatment and care of the data subject, or for the administration of the institution or professional practice concerned;

b) insurance companies, medical schemes, medical scheme administrators and managed healthcare organisations, if such processing is necessary for:

(i) assessing the risk to be insured by the insurance company or covered by the medical scheme and the data subject has not objected to the processing;

(ii) the performance of an insurance or medical scheme agreement; or

(iii) the enforcement of any contractual rights and obligations;

c) schools, if such processing is necessary to provide special support for pupils or making special arrangements in connection with their health or sex life;

d) any public or private body managing the care of a child if such processing is necessary for the performance of their lawful duties;

e) any public body, if such processing is necessary in connection with the implementation of prison sentences or detention measures; or

f) administrative bodies, pension funds, employers or institutions working for them, if such processing is necessary for—

(i) the implementation of the provisions of laws, pension regulations or collective agreements which create rights dependent on the health or sex life of the data subject; or

(ii) the reintegration of or support for workers or persons entitled to benefit in connection with sickness or work incapacity, and provided that such information is kept confidential;

7.2.8.11 where the processing concerns a person's criminal behaviour or biometric information, such processing is carried out by bodies charged by law with applying criminal law or by responsible parties who have obtained that information in accordance with the law, and where the processing concerns employees such processing is done in accordance with the rules established in compliance with labour legislation;

7.2.8.12 where the processing concerns a person under the age of 18, such processing is carried out with the prior consent of a competent person; or is necessary for the establishment, exercise or defence of a right or obligation in law; or is necessary to comply with an obligation of international public law; or for historical, statistical or

research purposes to the extent that—(i) the purpose serves a public interest and the processing is necessary for the purpose concerned; or(ii) it appears to be impossible or would involve a disproportionate effort to ask for consent, and sufficient guarantees are provided for to ensure that the processing does not adversely affect the individual privacy of the child to a disproportionate extent;

7.2.8.13 where the processing concerns special personal information, which has deliberately been made public by the child with the consent of a competent person.

7.2.9 Directors, employees and others processing personal information on behalf of the Organization must only process special personal information if it is able to justify such processing as described above. Processing special personal information without the data subjects' consent, or where such processing cannot be justified, may result in disciplinary action and in certain circumstances, may constitute a criminal offence, give rise to civil liability or administrative penalties.

7.3 Purpose specific

7.3.1 The Organization, including directors, employees and others processing personal information on behalf of the Organization, must only collect and process personal information for specified, explicit and legitimate purposes that have been communicated to data subjects before the personal information is collected.

7.3.2 When collecting and using a data subject's personal information, the Organization, including its directors, employees and others processing personal information on behalf of the Organization, have a duty to inform the data subject why the information is required and what will be done with it whilst under the Organization's control. Without a lawful basis and purpose for processing, such processing will be unlawful and unfair and may also have an adverse impact on the affected data subjects. No data subject should be surprised to learn that their personal information has been collected, consulted, used or otherwise processed by the Organization. In other words, any use or processing of a data subject's personal information must be purpose specific, and the data subject must be told about such processing and how such data will be used, before the intended use of the data. This accords with the universal data protection principles referred to under section 6 above, which state that the processing of a data subject's personal information will only be lawful if the data subject has been provided with an explanation for the processing, including the purpose, which has to be:

7.3.2.1 specific (not given in respect of multiple unrelated purposes);

7.3.2.2 informed (explained in plain and accessible language);

7.3.2.3 unambiguous and given by a clear affirmative action (meaning opt-in: silence, inactivity or pre-ticked boxes will not be sufficient);

7.3.2.4 separate and unbundled from any other terms and conditions provided to the data subject.

7.3.3 The Organization, it's Directors, employees and others processing personal information on behalf of the Organization must ensure that they do not process any personal information obtained for one or more specific purposes for a new purpose that is not compatible with the original purpose. If the Organization, or its directors, employees and others processing personal information on behalf of the Organization want to process additional personal information for a new purpose, which is not compatible with the original purpose for which the personal information was collected, then they will have to provide the data subject with the details of such processing and the reason(s) why the data has to be processed, and where necessary, if required, obtain the data subject's consent to such processing.

7.4 Data minimisation

7.4.1 The personal information that the Organization or its directors, employees and others processing personal information on behalf of the Organization collect and process must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is to be processed.

7.4.2 Directors, employees and others processing personal information on behalf of the Organization must only process personal information that is absolutely necessary for the performance of the required purpose and related duties and tasks and not for any other purposes. Accessing excessive personal information that is unnecessary or which one is not authorised to access, or that one has no reason to access, may result in disciplinary action and in certain circumstances, may constitute a criminal offence, give rise to civil liability or administrative penalties.

7.5 Accuracy

7.5.1 The personal information that the Organization, it's directors, employees and others processing personal information on behalf of the Organization collect and process must be accurate and, where necessary, kept up-to-date and must be corrected or deleted without delay when the Organization or its directors, employees and others processing personal information on behalf of the Organization discover, or are notified, that the data is inaccurate.

7.5.2 Directors, employees and others processing personal information on behalf of the Organization must ensure that they have procedures in place to ensure that the personal information on record is kept updated, especially where one becomes aware that personal information is inaccurate. Where appropriate, any inaccurate or out-of-date records should be deleted or destroyed.

7.6 Security, integrity and confidentiality

7.6.1 The personal information that the Organization, its directors, employees and others processing personal information on behalf of the Organization collect and process must be secured by appropriate technical and organisational measures which guard against accidental loss, destruction or damage, and against unauthorised or unlawful processing.

7.6.2 The Organization has developed, implemented and maintains appropriate technical and organisational measures for the processing of personal information taking into account the nature, scope, context and purposes for such processing, the volume of personal information processed and the likelihood and severity of the risks of such processing for the rights of data subjects and has procedures in place to ensure that it regularly evaluates and tests the effectiveness of such measures to ensure that they are adequate and effective.

7.6.3 Directors, employees and others processing personal information on behalf of the Organization must ensure that they:

7.6.3.1 observe and comply with all the Organization's information security policies, especially those pertaining to personal information security at all times;

7.6.3.2 do not attempt to circumvent any administrative, physical or technical measures the Organization has implemented as doing so may result in disciplinary action and in certain circumstances, may constitute a criminal offence, give rise to civil liability or administrative penalties;

7.6.3.3 ensure that the confidentiality and security of personal information is maintained at all times;

7.6.3.4 ensure that they only store personal information on Organization servers which are protected by approved security software, and one or more firewalls under the direction of the IT Manager and when transferred or uploaded to cloud computing services from computers, devices and applications, that these services have been approved by the IT Manager.

7.6.3.5 ensure that prescribed security measures and controls are implemented or where instructed followed to prevent all and any unauthorised access to personal information, the accidental deletion of personal information or the exposure of personal information to malicious hacking attempts;

7.6.3.6 ensure that all devices where personal information is stored, are password protected and that passwords are not written down or shared, irrespective of seniority or department, which passwords must be strong passwords which are changed regularly. If a password is forgotten, it must be reset using the applicable method;

7.6.3.7 ensure that all hardcopies of personal information, along with any electronic copies stored on physical or removable media is stored securely in a locked box, drawer, cabinet, or similar; and that such data is not removed from the Organization premises unless with prior approval from the IT department and when so removed, that such data is encrypted;

7.6.3.8 ensure that all personal information stored electronically is regularly

backed up using the Organization's provided systems and applications and in accordance with backup protocols. Such backups will be tested regularly in line with the Organization's standard backup procedures and protocols under the direction of the IT Manager;

7.6.3.9 ensure that no personal information is stored on any mobile device (including, but not limited to, laptops, tablets, smartphones or data sticks), whether such device belongs to the Organization or otherwise, without the formal written approval of the IT Manager and, in the event of such approval, the personal information is stored or held strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary when so stored, that such data is encrypted;

7.6.3.10 ensure that where personal information is stored on paper, that it is not left in places where persons can view the data, e.g., on a printer, but instead is kept in a secure place where an unauthorised person cannot access or see it, such as in a locked drawer, safe or cabinet and that when no longer required, that same is shredded;

7.6.3.11 ensure that when any personal information is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. For further information on the deletion and disposal of personal information, please refer to the Organization's Data Retention and Destruction Policy;

7.6.3.12 ensure that all device screens, when not in use are always locked especially when left unattended;

7.6.3.13 ensure that all personal information is only transmitted over secure networks, including wireless and wired networks;

7.6.3.14 ensure that personal information is not shared informally and when shared that there is a lawful or business reason for such sharing;

7.6.3.15 when sending emails which contain personal information, ensure that they are marked "confidential", do not contain the personal information in the body of the email, whether sent or received, but rather placed in an attachment, which email is then encrypted before being transferred electronically;

7.6.3.16 ensure that personal information is not transferred or sent to any entity not authorised directly to receive it;

7.6.3.17 ensure that personal information is not be kept in a form that identifies a data subject for longer than is necessary in relation to the purposes for which it was collected (except in order to comply with any legal, accounting or reporting requirements);

7.6.3.18 ensure that where personal information is to be sent by facsimile

transmission, ensure that the recipient has been informed in advance of the transmission and that he or she is waiting by the fax machine to receive the data;

7.6.3.19 ensure that where personal information is transferred physically, whether in hardcopy form or on removable electronic media ensure that it is passed directly to the recipient or sent using recorded deliver services and housed in a suitable container marked “confidential”;

7.6.3.20 ensure that generally all personal information is handled with care at all times, kept confidential, and that it is not left unattended or on view to unauthorised employees;

7.6.3.21 ensure that all software (including, but not limited to, applications and operating systems) used in connection with the Organization are installed on Organization owned computers or devices and which have been installed by and with the prior approval of the IT department, which software must at all times be kept up-to-date.

7.6.4 Retention of personal information

7.6.4.1 Storing personal information for longer than necessary may increase the severity of a data breach and may also lead to increased costs associated with such storage. In order to manage these risks, the Organization will maintain policies and procedures to ensure that personal information is deleted, destroyed or anonymised after a reasonable period of time following expiry of the purposes for which it was collected.

7.6.4.2 Directors, employees and others processing personal information on behalf of the Organization must take all reasonable steps to familiarise themselves with the Organization’s Records Management Policies and Data Retention and Destruction Policy and in line with this policy ensure that they create, manage, store, delete and / or destroy any personal information in accordance with the Organization’s Records Management Policies and Data Retention and Destruction Policy.

7.7 Sharing personal information

7.7.1 The transfer of any personal information to an unauthorised third party will give rise to and constitute a breach of the lawfulness, fairness and transparency principle and could give rise to liabilities and damages claims.

7.7.2 Directors, employees and others processing personal information on behalf of the Organization are not permitted to share personal information with third parties, unless:

7.7.2.1 there is a legitimate business need to share the personal

information;

7.7.2.2 the fact that the personal information will be shared with another has been communicated to the data subject in a privacy notice or processing notice beforehand;

7.7.2.3 the person receiving the personal information has either agreed to keep the personal information confidential and to use it only for the purpose for which it was shared under a data transfer agreement, or an Operator Agreement with the Organization, before receipt of the personal information.

7.8 Transfers outside of South Africa

7.8.1 POPIA prohibits the transfer of personal information outside of South Africa including transmitting, sending, viewing or accessing personal information, unless

7.8.1.1 the Information Regulator has issued an “adequacy decision” confirming that the territory or country to which the Organization proposes transferring the personal information to, has adequate personal information protection laws in place which will ensure that such data remains protected as it was in the country or territory from where it came;

7.8.1.2 the Organization has an approved set of standard binding corporate rules which apply to personal information which is transferred as between its own companies which make up its group, which companies are located in a territory or country which falls outside South Africa, which rules set out how the personal information will be protected as it was in the country or territory from where it came;

7.8.1.3 the Organization has a standard data transfer contract or Operator agreement in place which will be concluded with the third-party recipient of the personal information prior to them receiving personal information and which agreement houses the rules which will have to be followed by the third party in order to ensure that such data remains protected as it was in the country or territory from where it came;

7.8.1.4 the Organization has an approved code of conduct in place which has been approved by the Information Regulator which allows such transfers;

7.8.1.5 the data subject has given its express and explicit consent to the proposed transfer, having been fully informed of any potential risks;

7.8.1.6 the transfer is necessary in order to perform a contract between the Organization and a data subject, for reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the data subject in circumstances where the data subject is incapable of giving consent; or

7.8.1.7 the transfer is necessary, in limited circumstances, to protect the parties' legitimate interests.

7.8.2 Following the above, directors, employees and others processing personal information on behalf of the Organization are not permitted to transfer personal information to areas outside South Africa unless the person receiving the personal information has concluded a data transfer agreement or an Operator Agreement with the Organization, before receipt of the personal information, copies of which can be obtained from the Information Officer on request.

7.9 Transparency and processing notices

7.9.1 The Organization has a duty to show that it has dealt with a data subject in a transparent manner. In order to demonstrate transparency, the Organization must provide all data subjects with appropriate privacy notices or processing notices **before** it collects and processes their personal information.

7.9.2 POPIA sets out a detailed list of information that must be contained in all privacy notices and processing notices, including the types of personal information collected; the purposes for which they will be processed; the lawful basis relied upon for such processing; the period for which the personal information will be retained; who the Organization may share the personal information with; and, if the Organization intends to transfer personal information to countries outside South Africa, the mechanism relied upon for such transfer as well as the respective rights of the data subjects.

7.9.3 Whenever a director, employee and or any other representative processes personal information on behalf of the Organization, such person must ensure that data subject is made aware of the information set out below:

7.9.3.1 the types of personal information collected and the purpose or reason for the collection;

7.9.3.2 the lawful basis relied upon for such processing or whether consent is required for the processing;

7.9.3.3 the period for which the personal information will be retained;

7.9.3.4 who the Organization will be sharing the personal information with; including external transfers and the mechanism relied upon for such transfer;

7.9.3.5 the security measures which are in place to protect the data; and

7.9.3.6 the respective rights of the data subjects.

7.9.4 In order to streamline the above requirements, the Organization has developed and implemented a series of "processing notices" (informed consent notices)

which have to be presented to the various data subjects who the Organization engages with, including the following:

- employment processing notice;
- security and access control processing notice;
- service provider and vendor processing notice;
- recruitment processing notice;
- customer processing notice;
- website processing notice;
- general enquiry processing notice,

The notices are located on the Organization's website.

7.9.5 Directors, employees and / or any other representatives who processes personal information on behalf of the Organization, in order to give effect to the obligations set out under section 7.9.3 above, must ensure that all documents and / or records where personal information is recorded and / or housed or which calls for or sets out that personal information is required, must house a data processing clause which records or states in such document or record, that the Organization will have to, in order to deal with the data subject, process the data subject's personal information and that such processing is subject to:

7.9.5.1 the provisions of POPIA;

7.9.5.2 the Organization's processing notices;

7.9.5.3 where applicable, the Organization's standard binding corporate rules, its standard data transfer contract and / or Operator agreement.

7.9.6 The data processing clause referred to above should include the following information:

COMPLIANCE WITH PERSONAL INFORMATION PROCESSING LAWS

In terms of a variety of data privacy laws applicable around the world, including POPIA, where a person processes another's personal information, then in such an event, the person processing the personal information may only do so if such processing is lawful, legitimate and responsible and is done in accordance with the provisions of the data privacy laws, including POPIA. The Organization, in order to perform its business objectives, will have to process certain personal information which is owned or held by data subjects from time to time.

In order to comply with the provisions of these data privacy laws, including POPIA, the Organization must:

- *provide the data subject with a number of details pertaining to the processing of the data subject's personal information, before such information is processed, which details are housed under the*

Organization's Processing Notice, located on its website, which the data subject is requested to read;

- *obtain consent from the data subject to process its personal information, unless such processing: is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party; is required in order to comply with an obligation imposed by law; is necessary to protect or pursue the legitimate interest (s) of the data subject, the Organization or a third party to whom the personal information is provided to; or is necessary for the proper performance of a public law duty by a public body.*

The data subject hereby agrees to read the Processing Notice and in this regard consents to the Organization processing its personal information, save where such consent is not required as per the provisions of clause 7.2.3 above, the data subject accepting that the Organization is lawfully able to process such personal information without its consent.

Where the Organization provides personal information to another, who is tasked with Processing the personal information on behalf of the Organization in its capacity as an "Operator" as defined under POPIA, then in such case, the provisions set out under an Operator Agreement concluded will apply to such Processing, which terms will be incorporated into, and read together with this document."

7.10 Data subject rights and requests

7.10.1 POPIA provides data subjects with a number of rights in relation to their personal information, including the right to access its data, and to change it.

7.10.2 The Organization has developed, implemented and will maintain certain processes which give effect to these data subject rights, as described below, which processes will be directed to and handled directly by the Information Officer or his or her deputy, and no other.

7.10.3 All directors, employees and persons processing personal information on behalf of the Organization must take note of and give effect to these processes as described below.

7.10.4 The right to withdraw consent

7.10.4.1 Where a data subject has had to give its consent to the processing of its personal information, the data subject in such case will have the right to withdraw such consent at any time, which withdrawal will apply from the date of withdrawal only and which will not affect the legality of the processing of its personal information to which the consent applies prior to the withdrawal.

Information Officer Approval: Victor Southwell **Signed:**

7.10.4.2 In order to give notice of the withdrawal of consent, the data subject must complete the standard Organization "withdrawal of consent notice" housed on the Organization's website, which must be emailed to the Information Officer for further attention. Should the Information Officer give effect to such withdrawal, a stop processing notice will be sent to the affected director, employee or person processing such personal information on behalf of the Organization together with the consequences of such decision, who will then be required to stop the processing of the affected personal information.

7.10.5 The right to be informed

7.10.5.1 data subject has the right to be told why its personal information is being processed, including what type of personal information will be processed, the reason for the processing, who the personal information will be shared with and whether such information will be sent outside the territory where it is being processed or held, and how the personal information will be safeguarded.

7.10.5.2 In order to give effect to this right, the Organization has developed a series of processing or privacy notices which are described under section 7.9 above.

7.10.5.3 Directors, employees and / or any other representatives who process personal information on behalf of the Organization, in order to give effect to a data subject's right to be informed, must ensure that all documents and / or records where personal information is recorded and / or housed or which calls for or sets out that personal information or information is required, houses a data processing clause which records or states in such document or record, that personal information will be processed and that such processing is subject to the Organization's standard processing or privacy notices. An example of this clause is found under clause 7.9.6 above. The Organization's standard processing or privacy notices can be located on the Organization's website.

7.10.6 The data subject's right to have access to its personal information

7.10.6.1 All data subjects have the right at any time to ask any person or entity who holds its personal information, including the Organization, for access to their personal information, including finding out more about the personal information which the Organization holds about them, what it is doing with that personal information, and why it is processing the personal information.

7.10.6.2 In terms of POPIA, this right has to be exercised using the "request for access to information" procedure which is described under a law known as the Promotion of Access to Information Act, 2000 (PAIA) and which request procedure is more fully set out under the

Information Officer Approval: Victor Southwell **Signed:**

Organization's PAIA Manual.

7.10.6.3 All request for information held by the Organization, including personal information have to be made using the standard request procedure referred to under clause 7.10.6.2, which request will be submitted directly to, and which will be handled directly by, the Information Officer or his or her deputy, in accordance with the provisions of PAIA.

7.10.6.4 If any director, employee and / or any other representatives who processes personal information on behalf of the Organization is asked for any information which pertains to a data subject or to the Organization, such person making the request must be referred to the Information Officer or his Deputy, for further assistance.

7.10.7 Rectification of personal information

7.10.7.1 All data subjects have the right to request that their personal information is updated or rectified where it is inaccurate, incomplete or out of date. This request is set out under the Organization's prescribed "personal information update form", which form is housed on the Organization's website.

7.10.7.2 The Information Officer on receipt of the request, provided it is submitted on prescribed form, will where able, rectify so far as possible, the personal information in question, and inform the data subject of that rectification. Furthermore, in the event that any affected personal information has been disclosed to third parties, those parties will also be informed of any such rectification and the reasons therefor.

7.10.8 The right to object and / or restrict processing

7.10.8.1 Data subjects have the right to object to the Organization processing their personal information based on legitimate interests, direct marketing (including profiling), and processing for scientific and/or historical research and statistics purposes.

7.10.8.2 Where a data subject objects to the Organization processing its personal information based on its legitimate interests, the Organization shall cease such processing immediately, unless it can be demonstrated that the Organization has legitimate grounds for such processing which override the data subject's interests, rights, and freedoms, or that the processing is necessary for the performance of a legal or statutory duty or the conduct of legal claims.

7.10.8.3 Where a data subject objects to the Organization processing its personal information for direct marketing purposes, the Organization must immediately stop any further direct marketing.

7.10.8.4 A data subject furthermore has the right to object to the processing

of its personal information coupled with the right to ask the Organization to restrict processing the personal information where the data subject:

7.10.8.4.1 believes that the personal information is inaccurate;

7.10.8.4.2 believes that the processing was unlawful and the data subject prefers restriction of processing over erasure;

7.10.8.4.3 believes that the personal information is no longer necessary in relation to the purposes for which it was collected but one is required to establish, exercise or defend a legal claim and needs to retain the data; or

7.10.8.4.4 has objected to the processing pending a determination whether the Organization's legitimate interest's grounds for processing the personal information override those of the data subject.

7.10.8.5 In accordance with the above, the data subject may object to, and ask the Organization to place a restriction on the processing of the personal information which the Organization holds, which request has to be made to the Information Officer or his or her deputies for determination and action.

7.10.8.6 If the Information Officer is in agreement with and succumbs to the request of the data subject, then the Organization shall pend any further processing of the personal information in question and retain only the amount of personal information concerning that data subject (if any) that is necessary to ensure that the personal information in question is not processed further.

7.10.8.7 In the event that any affected personal information has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

7.10.9 The right to data portability

7.10.9.1 This is the right of the data subject to receive or ask the Organization to transfer to a third party, a copy of the data subject's personal information in a structured, commonly-used machine-readable format.

7.10.9.2 To facilitate the right of data portability, the data subject must complete the "data portability" prescribed request form which form is housed on the Organization's website and submit same to the Information Officer or his deputy who will attend to and where possible facilitate the request if technically feasible.

Information Officer Approval: Victor Southwell **Signed:**

7.10.10 The right to object to direct marketing

7.10.10.1 A data subject who has opted into any form of direct marketing has the right to opt out from any subsequent direct marketing, i.e., it has the right to ask the Organization not to process its personal information for any further direct marketing purposes.

7.10.10.2 A data subject can either submit its request using the prescribed objection notice (see notice referred to under section 7.10.8.5) or alternatively simply use the opt out request which the Organization is obliged to include in all its electronic direct marketing communications.

7.10.11 The right to object to decisions based solely on automated processing including profiling

7.10.11.1 A data subject has the right to object to decisions creating legal effects or significantly affecting the data subject which were made solely by automated means, including profiling, and the right to request human intervention. The data subject also has the right to ask for the reasons why a decision was made and the underlying methodology which was used to make the decision which request must be made by completing and submitting the prescribed "automated objection" notice, which is housed on the Organization's website.

7.10.12 The right to erasure (right to be forgotten)

7.10.12.1 A data subject has the right to request that the Organization erases the personal information which the Organization holds about it in the following circumstances: it is no longer necessary for the Organization to hold that personal information with respect to the purpose(s) for which it was originally collected or processed; the data subject wishes to withdraw its consent; the data subject objects to the Organization holding and processing its personal information (and there is no overriding legitimate interest to allow the Organization to continue doing so); the personal information has been processed unlawfully; or personal information needs to be erased in order for the Organization to comply with a particular legal obligation.

7.10.12.2 The request for erasure must be submitted using the "request for erasure" prescribed form, which is housed on the Organization's website, which request will be handled and a subsequent decision made, by the Information Officer and / or his or her deputies.

7.10.12.3 Unless the Organization has reasonable grounds to refuse to erase

Information Officer Approval: Victor Southwell **Signed:**

personal information, all requests for erasure shall be complied with, and the data subject must be informed of the erasure, if the request is valid and feasible.

7.10.12.4 In the event that any personal information that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

7.10.13 The right to be notified of a personal information breach

7.10.13.1 A data subject must be notified of a personal information breach which involves its personal information, which notice will be prepared by and conveyed to affected data subjects by the Information Officer. This procedure is described under section 15.18 below.

7.10.13.2

7.10.14 The right to complain

7.10.14.1 A data subject has to right lodge a complaint with regards to the processing of its personal information, which compliant must set out and concern a non-compliance by the Organization with the data processing principles or concern a non-compliance with POPIA.

7.10.14.2 The data subject is encouraged to make use of the Organization's internal complaint resolution procedures, and submit its complaint to the Information Officer.

7.10.14.3 On receipt of the compliant the Information Officer will attempt to hear and resolve the matter, and failing resolution will provide the data subject with a non-resolution notice.

7.10.14.4 If the Information Officer and data subject are able to resolve the matter, a record setting out the solution will be compiled, and signed by the parties and any other affected persons provided with details of the resolution.

7.10.14.5 Where the parties are unable to resolve the matter, the data subject on receipt of the non-resolution notice will have the right to refer the compliant onwards, in the case of an alleged POPIA breach or infringement, to the Information Regulator.

7.10.15 In order to give effect to the above, all directors, employees and / or any other representatives who processes personal information on behalf of the Organization, must familiarise themselves with these rights and the related processes, and ensure that all data subjects are informed of these rights and the procedures which have to be followed when a data subject wishes to make use of these rights.

7.11 Data Protection Impact Assessments

Information Officer Approval: Victor Southwell **Signed:**

7.11.1 A Data Protection Impact Assessment (DPIA), also known as a Privacy Impact Assessment, is a process to help identify and minimise the data protection risks involved in projects, processes and activities involving the processing of personal information.

7.11.2 In order to assess the impact of the data privacy laws, and what the Organization needs to do in order to comply with these laws, an initial base line (DPIA) will be conducted by the Information Officer and his or her deputies and which will form the basis of the Organization's data privacy framework.

7.11.3 Further DPIA's will be carried out when new technologies or new systems, solutions and research studies are implemented or where personal information processing is likely to result in high risk to both the data subjects and to the Organization.

7.11.4 DPIA must:

7.11.4.1 describe the nature, scope, context and purposes of the processing;

7.11.4.2 assess necessity, proportionality and compliance measures;

7.11.4.3 identify and assess risks to individuals;

7.11.4.4 identify any additional measures to mitigate those risks.

7.11.5 Without exception all DPIAs must be assessed and signed off by the Information Officer and, where relevant, IT Services.

7.11.6 In order to give effect to the above, all directors, employees and / or any other representatives who process personal information on behalf of the Organization must familiarise themselves with the requirement to conduct a DPIA and ensure where one is required that it is conducted in accordance with the Organization's DPIA Policy.

7.12 Direct marketing

7.12.1 The Organization and its directors, employees and / or any other representatives who processes personal information on behalf of the Organization must ensure that before they send direct marketing to customers for the first time, that they have given the customer the opportunity in an informal manner to agree or disagree to the receipt of direct marketing material.

7.12.2 The Organization and its directors, employees and / or any other representatives who process personal information on behalf of the Organization must ensure that before they send direct marketing to non-customers that they receive appropriate "opt in" consents in the prescribed manner and form as per the provisions of POPIA, which form is housed on the Organization's website.

7.12.3 The Organization and its directors, employees and / or any other representatives

Information Officer Approval: Victor Southwell **Signed:**

who process personal information on behalf of the Organization must ensure that when a data subject exercises their right to object to direct marketing, in the form of an “opt out” that such opt out is recorded and honoured.

7.12.4 The Organization has developed a direct marketing policy and guideline and all directors, employees or persons who process personal information on behalf of the Organization, must familiarise themselves with these documents and ensure that they understand and comply with these obligations in relation to direct marketing before embarking upon any direct marketing campaign.

7.13 Operators

7.13.1 An operator is an entity who processes personal information on behalf of the Organization without coming under its direct control.

7.13.2 All operators and processors have to conclude the Organization’s standard data transfer contract or Operator Agreement prior to them receiving and or processing personal information on behalf of the Organization, which agreement houses the rules which will have to be followed by the operator or processor in order to ensure that such data is processed and protected in accordance with the processing laws and the Organization’s security procedures and standards.

7.13.3 Directors, employees or persons who process personal information on behalf of the Organization, must ensure that when they appoint an operator that the relevant standard data transfer contract or Operator Agreement is concluded with such operator or processor prior to them receiving and or processing personal information on behalf of the Organization.

7.14 Profiling

7.14.1 The Organization does from time to time, use personal information for profiling purposes which is done via “cookies” on its web sites.

7.14.2 Directors, employees or persons who process personal information on behalf of the Organization, must ensure that when personal information is used for profiling purposes, that the following takes place:

7.14.2.1 clear information explaining the profiling is provided to data subjects, via privacy notices, cookie opt ins and cookie notices, including the significance and likely consequences of the profiling;

7.14.2.2 appropriate mathematical or statistical procedures are used;

7.14.2.3 technical and organisational measures are implemented to minimise the risk of errors. If errors occur, such measures must allow the errors to be easily corrected;

7.14.2.4 All personal information processed for profiling purposes shall be secured in order to prevent discriminatory effects arising out of profiling.

7.15 Training

7.15.1 The Organization will conduct regular training sessions covering POPIA and the Organization's related personal information processing policies and procedures, which will be available to all directors, employees and / or persons who process personal information on behalf of the Organization.

7.15.2 All directors, employees and / or persons who process personal information on behalf of the Organization, must ensure that they have undertaken the necessary training, that they understand the privacy laws and the Organizations related personal information processing policies and procedures, and that importantly all processing of personal information is done in accordance with POPIA, the training, the related policies and procedures and / or any guidelines issued by the Organization from time to time.

7.16 Record-keeping

7.16.1 The Organization must keep full and accurate records of all its processing activities in accordance with POPIA and related requirements including:

7.16.1.1 the name and details of the Information Officer and any deputies appointed in South Africa;

7.16.1.2 all processors and / or operators who process personal information on behalf of the Organization;

7.16.1.3 the purposes for which the Organization collects, holds, and processes personal information;

7.16.1.4 details of the categories of personal information collected, held, and processed by the Organization;

7.16.1.5 details of any transfers of personal information to non-South African operations situated in countries outside South Africa, including all mechanisms and security safeguards;

7.16.1.6 details of all retention periods in respect of personal information as per the Records Management and Retention Policies and Records Retention Schedule; and

7.16.1.7 detailed descriptions of all technical and organisational measures taken by the Organization to ensure the security of personal information.

7.17 Archiving and destruction of data

7.17.1 The Organization in order to facilitate the correct creation, use, storage, archive, retrieval and ultimate destruction of records has developed a set of Records Management and Retention Policies and Records Retention Schedule.

7.17.2 Directors, employees and others processing personal information on behalf of the

Information Officer Approval: Victor Southwell **Signed:**

Organization must ensure that when they process personal information, that such data is processed in strict compliance with the Organization's Records Management and Retention Policies and Records Retention Schedule.

7.17.3 Directors, employees and others processing personal information on behalf of the Organization must furthermore ensure that when personal information is no longer needed for the specific purposes for which it was collected, that such personal information is archived for the legally required retention period and thereafter deleted, destroyed or anonymised, which must be done is strict compliance with the Organization's Retention Policies and Records Retention Schedule.

7.18 Reporting personal information breaches

7.18.1 In the event of a personal information breach, the Organization has a duty to give notice of such breach to the Information Regulator in the case of a breach in South Africa, and the affected data subjects.

7.18.2 The Organization has put in place appropriate procedures to deal with any personal information breach and will notify the Information Regulator and/or the data subjects as the case may be when it is legally required to do so.

7.18.3 All cyber and or data breaches, including ones which involve personal information are strictly private and confidential.

7.18.4 All personal information breaches must be reported immediately to the Organization's Information officer, which report must include the following details:

7.18.4.1 categories and approximate number of data subjects concerned;

7.18.4.2 categories and approximate number of personal information records concerned;

7.18.4.3 the likely cause of and the consequences of the breach;

7.18.4.4 details of the measures taken, or proposed to be taken, to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

7.18.5 Only the Information Officer with the approval of the Organization's Board has the right to report any personal information or security breach to the Information Regulator and / or the affected data subjects, as the case may be.

7.18.6 Directors, employees and / or any other representatives who processes personal information on behalf of the Organization must familiarise themselves with, observe and comply with the Organization's personal information breach procedure and to this end has a duty to immediately report through to the Information Officer, any known or suspected data breach and to take all appropriate steps to preserve evidence relating to the breach.

Information Officer Approval: Victor Southwell **Signed:**

8. GOVERNANCE

8.1 Information Officers and deputies

8.1.1 The Organization has appointed an Information Officer.

8.1.2 The Information Officer has the right to appoint and to delegate certain activities to deputy Information Officers.

8.1.3 the Information Officer will be responsible for the following:

8.1.3.1 developing, constructing and once prepared, implementing and overseeing an enterprise-wide personal information processing framework and related roadmap;

8.1.3.2 developing, constructing and once prepared, implementing and overseeing the various personal information processing policies and procedures, including this Policy;

8.1.3.3 monitoring compliance with this Policy, the various personal information processing policies and POPIA;

8.1.3.4 arranging and implementing data protection training to all directors, employees and other persons who process personal information on behalf of the Organization;

8.1.3.5 providing on going guidance and advice on personal information processing;

8.1.3.6 conducting personal information impact assessments (PDIA's) when required, including base line risk assessments of all the Organization's personal information processing activities;

8.1.3.7 ensuring that all operational and technological data protection standards are in place and are complied with;

8.1.3.8 working closely with IT in order to ensure that appropriate technological and operational measures have been implemented in order to ensure the safety and security of all personal information which the Organization holds;

8.1.3.9 receiving and considering reports from IT about compliance with all technological and operational data protection standards and protocols;

8.1.3.10 be entitled and have authorisation to initiate disciplinary proceedings

Information Officer Approval: Victor Southwell **Signed:**

against any employee who at any time breaches any technological and/or organisational and/or operational data protection standard, rule, custom, instruction, policy, practice and/or protocol (verbal, in writing or otherwise) ("rule") applicable in any department or area of the operations of the Organization;

8.1.3.11 review and approve any contracts or agreements with third parties to the extent that they may handle or process data subject information;

8.1.3.12 attend to requests and queries from data subjects in respect of their respective data subject rights detailed under section 7.9 of this Policy, including requests for access to their personal information;

8.1.3.13 liaising with and / or co-operating with any regulators or investigators or officials who may be investigating a data privacy matter.

8.2 IT Manager

8.2.1 The Organization has appointed an IT Management Company.

8.2.2 The IT Management Company has the right to appoint and to delegate certain activities to deputy IT personnel.

8.2.3 The IT Manager will be responsible for the following:

8.2.3.1 conducting cyber security risk assessments including base line risk assessments of all the Organization's information technology activities;

8.2.3.2 ensuring that adequate and effective IT operational and technological data protection procedures and standards are in place in order to address all IT security risks;

8.2.3.3 ensuring that all systems, services and equipment used for processing and/or storing data adheres to internationally acceptable standards of security and data safeguarding, and is regularly updated to continue to comply with such standards;

8.2.3.4 issuing appropriate, clear, and regular rules and directives, whether for the Organisation as a whole or a particular part of it, department, person or level of person in relation to any aspect of the Organization's work, including password protocols, data access

Information Officer Approval: Victor Southwell **Signed:**

protocols, levels of persons who enjoy access to certain data sign-on procedures, password safeguarding protocols, sing-on and sign-off procedures, log-on and log-off procedures; the description of accessories, applications and equipment that will or may be used, and/or that may not be used under any circumstances, and the like.

8.2.3.5 evaluate any third-party services the Organization is considering or may acquire to process or store data, e.g., cloud computing services and ensuring that appropriate and effective operational and technological data protection procedures and standards are in place in order to address all IT security risks which may present themselves in respect of these external service providers.

9. RELATED POLICIES & PROCEDURES

This Policy forms part of a broader Information Governance Framework with other policies, guidance notes and procedures maintained by the Organization.

10. NON-COMPLIANCE

Compliance with this POPIA Policy or any of the policies, guidance notes and procedures referred to under clause 7 are mandatory and breach of any of the requirements contained therein may result in disciplinary action and / or possible criminal and / or civil action.

11. VERSION AND AMENDMENTS

This Policy is effective as of 30 June 2021.

Information Officer Approval: Victor Southwell **Signed:**

Information Officer Approval: Victor Southwell

Signed: 

SCHEDULE 1 - GLOSSARY

Automated processing	Any form of processing (including profiling) that is undertaken by automated means to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning their performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements
Consent	Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the processing of personal information about them
Responsible party (POPIA)	The person or organisation that determines the purposes and means of processing personal information
Criminal convictions and offences	Personal information relating to criminal convictions, the commission or alleged commission of an offence, proceedings for the commission or alleged commission of an offence and sentencing
Data protection impact assessment (DPIA)	A tool used to identify and reduce the risks of a processing activity, also known as 'Privacy Impact Assessments.
POPIA / Data privacy law	The Protection of Personal Information Act, 14 of 2013 (POPIA)
Data subject	An individual or legal entity (POPIA) to whom personal information relates and who can be identified or is identifiable from personal information
Information Officer (IO) (POPIA)	A person required to be appointed under POPIA and who must have expert knowledge of data protection law and practice, being the organisation's main representative on data protection matters
Processing notices	A notice setting out information that must be provided to data subjects before collecting personal information from them, including notices aimed at a specific group of individuals or notices that are presented to a data subject on a 'just- in-time' basis (also known as 'privacy notice' or 'data protection notices')
Personal information breach	A breach of security lead to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information transmitted, stored or otherwise processed and which compromises the confidentiality, integrity, availability and/or security of the personal information

Information Officer Approval: Victor Southwell **Signed:**

Personal information	Any information identifying a data subject or information relating to a data subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal information includes criminal convictions and offences data, special categories of personal information and pseudonymised personal information but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal information can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour
Privacy notices	See processing notices above
Process, processes, processing	Any activity or set of activities which involves personal information including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or making available, alignment or combination, restriction, erasure or destruction
Processing areas	South Africa
Pseudonymised, pseudonymisation	Replacing information that directly or indirectly identifies an individual with one or more artificial identifiers (for example, a numerical identifier or other code) or pseudonyms so that the data subject cannot be identified without combining the identifier or pseudonym with other information which has been kept separately and securely. Personal information that has been pseudonymised is still treated as personal information (unlike personal information which has been anonymised)
Related policies and procedures	The related POPIA policies and procedures
Special categories of personal information	Means information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and, for the purposes of this policy personal information relating to criminal offences and convictions.

Information Officer Approval: Victor Southwell **Signed:**