UMBHABA ECO LODGE (PTY) LTD

Protection of Personal Information Act 4 of 2013

DATA PROTECTION POLICY

2021

This is a confidential document not for dissemination or use outside the company.

RECORD

Version	Date	Submitted to	Status
1	1 July 2021	Directors	Approved

INTERNAL POPIA POLICY

NOTICE: THIS POLICY IS FOR INTERNAL USE ONLY. THIS POLICY IS NOT AVAILABLE FOR DISTRIBUTION TO THE PUBLIC OR ANY THIRD PARTY WITHOUT PRIOR APPROVAL OF THE INFORMATION OFFICER OF THE COMPANY.

1. OVERVIEW

1.1. Introduction to the Act

1.1.1. The right to privacy forms the cornerstone of information and data protection laws worldwide. Similarly, the Protection of Personal Information Act 4 of 2013, as amended from time to time ("**POPIA**") aims to protect the constitutional right to privacy in South Africa. Information and data protection have become a global issue and stringent protection thereof is now the international norm.

1.1.2. POPIA was enacted with the intention of establishing, enhancing and modernising the South African framework governing the Processing of Personal Information and to bring South African legislation in line with the approaches of the international community.

1.1.3. The enactment of POPIA means that we are attempting to align our privacy and data protection laws in line with acceptable global standards. POPIA is in fact based on the formation and data protection laws of the European Union, which like South Africa, base their laws on a human rights foundation.

1.1.4. The primary objective of POPIA is to promote the constitutional right to privacy, which is enshrined in section 14 of the Constitution.

1.2. Primary objectives of the Act

1.2.1. As its most important aim, POPIA strives to protect personal information and ensure its confidentiality by regulating the way in which such information is generally collected, stored, used and even destroyed.

1.2.2. It does so by introducing certain minimum measures or requirements in terms of which personal information must be processed, and requiring that entities and persons who receive such personal details and information implement reasonable measures to ensure that personal information is processed in a manner which –

1.2.2.1. is fair and responsible;

1.2.2.2. is conducted in a secure manner; and

1.2.2.3. aims to ultimately ensure that such personal information remains private and confidential.

1.2.3. POPIA also provides remedies to those whose right to privacy and data security has been infringed in order to protect persons from suffering damage and harm due to misuse of their personal information.

1.2.4. In summary, the Act therefore aims to regulate the manner in which Personal Information is Processed, as well as to combat misuse of the Personal Information of Data Subjects. POPIA accordingly imposes obligations on Operators and Responsible Parties who Process the Personal Information of Data Subjects to ensure that such organisations comply with the provisions of the Act.

1.3. **POPIA effective date**

POPIA was signed into law on 19 November 2013, but the majority of the provisions only came into effect on 01 July 2020. This means that POPIA is now operational and that its provisions apply to the processing of personal information and data going forward.

1.4. **Application of the Act to the Company**

The "**Company**" (as defined in paragraph 3) qualifies as a Responsible Party contemplated in Chapter 1 of the Act and therefore implements this internal POPIA Policy (as defined in paragraph 2) to establish clear procedures for the Company to comply with the provisions of the Act.

2. PURPOSE

2.1. This document represents the formulation and implementation of a data protection policy, depicting the internal procedures and policy of the Company as required in terms of POPIA.

2.2. The Compliance Framework aims to set out the obligations, applicable procedures and time frames for every professional and support staff member who falls within the ambit of the Act.

2.3. This Policy must be read with any and all other documents, manuals and guidance documents of the Company pertaining to the Act.

3. DEFINITIONS

In this Policy, unless the context otherwise requires, the following capitalised terms shall have the meanings assigned to them below and cognate expressions shall have corresponding meanings:

"**Company**"	means Umbhaba Eco Lodge (PTY) Ltd with registration number 2019/211155/07,
"**Compliance Framework**"	the framework established in terms of this Policy of the Company and detailed in paragraph 7 (*Compliance Framework*), and which is aimed at promoting and ensuring compliance by the Company with its obligations in terms of the Act;
"**Constitution**"	the Constitution of the Republic of South Africa of 1996;

"**Data Subject**"	a person to whom Personal Information relates and is therefore the party whose Personal Information is Processed by Responsible Parties. Data Subjects include identifiable, living natural persons and if applicable, an identifiable existing juristic person, to whom Personal Information may relate;
"**Data Breach**"	means any unauthorised access to the Personal Information of Data Subjects in the possession or under the control of the Company or an Operator used by the Company;
"**Employee(s)**"	all professionals and support staff members of the Company who may engage in or facilitate the Processing of Personal Information;
"**Information Officer**"	means the individual who will be responsible, within an entity or institution, for ensuring compliance with POPIA and being responsible for the governance, management and security of Personal Information, as required in terms of POPIA and as more comprehensively defined in the Act, and any reference to "**Information Officer**" shall also constitute a reference to a duly appointed "**deputy information officer**" as contemplated in terms of POPIA;
"**Information Regulator**"	means the statutory body that is responsible for the enforcement and implementation of POPIA and which has been bestowed with extensive powers in terms of the Act, including the power to receive and investigate complaints, impose sanctions and publish guidelines and guidance documents in terms of POPIA compliance requirements;
"**Operator**"	any person or entity that Processes Personal Information on behalf of a Responsible Party in terms of a contract or mandate, without falling under the direct authority of the Responsible Party;
"**Personal Information**"	any information relating to an identifiable, living natural person and if applicable, to an existing identifiable juristic person, and which includes general Personal Information and Special Personal Information (as the relevant context and circumstances may require);
"**Policy**"	means this internal POPIA policy which applies to the Company and all its employees as set out in paragraph 3 (*Scope*) below;
"**POPIA / the Act**"	the Protection of Personal Information Act 4 of 2013, as may be amended, substituted or varied from time to time;
"**Processing**"	the processing of Personal Information involves any collection, use, storage, deletion or destruction of Personal Information. The processing of Personal Information is of an ongoing nature and compliance with the provisions of

POPIA must be in place for as long as the Personal Information is being processed and stored, and "**Process**" and "**Processed**" in this context shall have a corresponding meaning;

"**Responsible Party**" means the party responsible for ensuring compliance with POPIA when Processing Personal Information, and encompasses any public or private bodies or any other person that either alone or together with others, determines the purpose of and means for Processing Personal Information, and "Responsible Parties" shall have a corresponding meaning;

"**Senior Management**" means the board of directors of the Company from time to time;

"**Special Personal Information**" means Personal Information concerning –

(i) the religious or philosophical beliefs;

(ii) race or ethnic origin;

(iii) trade union membership;

(iv) political persuasion;

(v) health or sex life; or

(vi) biometric information (which includes information that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition),

of a Data Subject; or

(vii) the criminal behaviour of a Data Subject to the extent that such information relates to –

a. the alleged commission by a Data Subject of any offence; or

b. any proceedings in respect of any offence allegedly committed by a Data Subject or the disposal of such proceedings;

"**Technical and Organisational Security Measures**"	means those appropriate, reasonable, technical and organisational measures aimed at protecting the integrity and confidentiality of Personal Information against loss of, damage to or unauthorised destruction and unlawful access to and against all other unlawful forms of Processing, and includes any generally accepted information security practices and procedures which may apply generally or be required in terms of specific industry or professional rules and regulations.

4. SCOPE

4.1. This Policy applies to all our Employees (including temporary, fixed-term, and permanent employees), consultants, contractors, trainees, seconded staff, home workers, casual workers, agency staff, volunteers, interns, agents, sponsors, or any other person or persons associated with us (including third parties), no matter where they are located. The Policy also applies to all directors, board members, and/or shareholders at any level.

4.2. Compliance with the provisions of this Policy is mandatory and failure to do so can result in severe consequences for the Company and the individuals concerned.

4.3. This Policy –

4.3.1. sets out the minimum standards to which all Employees of the Company must adhere to at all times;

4.3.2. exists in order to set out the responsibilities of all parties to whom this Policy applies;

4.3.3. serves as a source of information and guidance for those to whom it applies on how to deal with the Processing of Personal Information; and

4.3.4. provide information and guidance to our Employees on how to deal with a Data Breach.

5. POLICY IMPLEMENTATION

5.1. We provide training to all employees whom holds and/or process information, pertaining to what the acceptable and unacceptable practices are in relation to this Policy.

5.2. Such training is compulsory for all our Employees whom holds and process information and no employee may be excused from such training. The training shall include an in-depth discussion and explanation of this Policy.

5.3. Please take note that failure to comply with this Policy may lead to Employees being subject to disciplinary action, up to and including dismissal.

6. LEGAL FRAMEWORK

6.1. Introduction

In order to fully understand our compliance obligations in terms of POPIA, it is first important to understand the various concepts, role players, structure and framework that make up these obligations. These are discussed in further detail below.

6.2. Important concepts

6.2.1. *Personal Information*

6.2.1.1. POPIA describes Personal Information as any information relating to an identifiable, living natural person and if applicable, to an existing identifiable juristic person. Personal information may thus include the following:

6.2.1.1.1. Information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of a person.

6.2.1.1.2. Information relating to the education or the medical, financial, criminal or employment history of a person.

6.2.1.1.3. Any identifying number (such as an identity number or passport number), symbol, electronic mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person.

6.2.1.1.4. The personal opinions, views or preferences of the person. These constitute rather broad concepts and may encompass a wide range of information relating to a person.

6.2.1.1.5. Correspondence (such as by means of electronic mail or letter) sent by a person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence.

6.2.1.1.6. The views or opinions of another individual about a person.

6.2.1.1.7. The name of a 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.

6.2.1.2. Personal Information that is Processed should be distinguished, so that it is clear what information applies to which Data Subject. Accordingly, Responsible Parties should make use of effective and efficient record keeping practices that allow this correlation between data and Data Subjects.

6.2.2. In light of the broad nature of the concept of Personal Information, if and when the Company requires customers, clients and other third parties to provide us with Personal Information, such as their name, identity

number, residential address and contact details, we will be Processing Personal Information.

6.2.3. POPIA distinguishes two categories of Personal Information, namely general Personal Information and so-called Special Personal Information. While the first category is broad enough to potentially extend to all Personal Information, the second category provides for various categories of sensitive Personal Information, which as a general rule, may not be Processed in the absence of certain requirements, which includes the consent of the Data Subject.

6.2.4. Special Personal Information is regarded as sensitive, in light of the fact that misuse of these categories of information has the potential to severely and adversely affect the rights of Data Subjects, especially their rights to privacy and non-discrimination. The misuse of Special Personal Information may result in long term consequences, which adversely affects Data Subjects in relation to their social and occupational environment and development.

6.2.5. Although Special Personal Information may generally not be Processed, such Processing may be justified and lawful if one of the exceptions listed in POPIA apply to the circumstances. These exceptions include the following:

6.2.5.1. The Data Subject has consented to the Special Personal Information being Processed.

6.2.5.2. The Processing is necessary for the establishment, exercise or defence of any right or obligation required by law.

6.2.5.3. The Processing is necessary in order to comply with an obligation of international public law.

6.2.5.4. Processing is for historical, statistical or research purposes to the extent that it serves a public interest and the processing is necessary for that purpose, or it appears to be impossible or would involve an unreasonable effort to obtain consent, and sufficient guarantees are provided to ensure that the Processing does not adversely and disproportionately affect the individual privacy of the Data Subject.

6.2.5.5. The information has deliberately been made public by the Data Subject. The key factor here is the intention of the Data Subject that the information should have been made public. The fact that Special Personal Information is contained in a public record does not automatically illustrate that the Data Subject wanted the information to be made public and consequently cannot be Processed under this exemption.

6.2.5.6. It is noteworthy to keep in mind that the Processing of the Personal Information of children is prohibited, unless expressly authorised in terms of POPIA. This strict prohibition aims to advance the best interests of children in terms of the Constitution. The exceptions for Processing of this information are the same as for Special Personal Information, save for the fact that consent for Processing should be obtained from a competent person such as a parent or legal guardian.

6.2.6. *Processing*

6.2.6.1. In terms of POPIA, the Processing of Personal Information involves any collection, use, storage, deletion or destruction of Personal Information. The Processing of Personal Information is of an ongoing nature and compliance with the provisions of POPIA must be in place for as long as the personal information is being Processed (including when and for the entire time that such information is stored).

6.2.6.2. POPIA applies to the Processing of all Personal Information by or for a Responsible Party by automated (*namely electronic*) or non-automated (*non-electronic*) means.

6.2.6.3. In the event that Personal Information is Processed by automated means, which includes all electronic sources, it must be entered into a "**record**" by or for the Responsible Party. A record is described broadly in terms of POPIA and includes all recorded information, irrespective of the form or medium of such information. POPIA requires that a record must be in the possession or under the control of a Responsible Party, irrespective of whether it was created by the Responsible Party and regardless of when it came into existence. A record may be any of the following:

6.2.6.3.1. Writing on any material.

6.2.6.3.2. 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.

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

6.2.6.3.4. A book, map, plan, graph or drawing.

6.2.6.3.5. A 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.

6.2.6.4. In the event that the Personal Information is processed by non-automated means, for example paper, text and other hard copy sources, it must be entered into a record by or for the Responsible Party and form part of a filing system or must be intended to form part of a filing system. By implication, if Personal Information held in a physical form is not filed as part of a filing system, or is not intended to be filed as part of a filing system, then POPIA will not apply.

6.2.7. *Sharing and outsourcing of Personal Information*

6.2.7.1. Responsible Parties will often, for a variety of reasons, wish to share Personal Information under their possession and control with third parties. For example, Responsible Parties may want to share Personal Information for certain operational reasons, between their related and inter-related business entities. Such sharing of Personal Information may be rendered POPIA compliant if the Data Subject is informed of this fact and consents to the sharing of their Personal Information.

6.2.7.2. Responsible Parties may also wish to outsource the Processing of Personal Information to third party operators who further Process the Personal Information on behalf of the Responsible Party for the payment of a fee. Operators generally include, amongst others, various service providers, businesses such as payroll companies, telemarketing companies or businesses that conduct customer satisfaction surveys, process research data or store and administer information.

6.2.7.3. The sharing of Personal Information with Operators is permissible provided that all the requirements for outsourcing of the Personal Information to an Operator in terms of POPIA are met.

6.2.7.4. It is important to note that the outsourcing of Personal Information to an Operator does not release the Responsible Party from its obligations in terms of POPIA. If the Operator contravenes POPIA in any way, the Responsible Party will still be held accountable.

6.2.7.5. It is therefore advisable that a proper Operator agreement be concluded between the relevant parties before any data processing is outsourced. The conclusion of a written agreement in this regard should be discussed with the Information Officer should same be required or relevant in accordance with the circumstances.

6.3. **The role players**

It is important to distinguish between the different role players in terms of POPIA, since the same person or entity can be a different role player (Data Subject, Responsible Party or Operator) under different circumstances. Knowing what role player the Company is under such varying circumstances has an impact on our responsibilities and potential liability.

6.3.1. *The Data Subject*

6.3.1.1. POPIA identifies the Data Subject as the person to whom Personal Information relates and is therefore the party whose Personal Information is Processed by Responsible Parties.

6.3.1.2. Data Subjects include identifiable, living natural persons and if applicable, an identifiable existing juristic person, to whom personal information may relate.

6.3.1.3. It is important to note two main considerations from this definition, firstly that deceased persons cannot qualify as Data Subjects in terms of POPIA and secondly, that the Data Subject must be identifiable. Accordingly, if the Personal Information of a Data Subject has been de-identified then POPIA will not apply. This may be relevant in circumstances where the identifying information, such as a name and identity number of persons who participated in a survey is redacted or removed from a questionnaire form and only their answers are used, stored or further Processed.

6.3.1.4. A Data Subject will accordingly be the party that will provide a particular business or institution with their identifying and Personal Information.

6.3.1.5. In determining who is a Data Subject, it is important to remember that a Data Subject must be

identifiable. Persons are considered to be identifiable if they can be distinguished and differentiated from other persons through their Personal Information, such as their name, identity number, car registration or residential address. Data Subjects may also be identified on the basis of their indisputable biological characteristics and their psychological and behavioural traits.

6.3.1.6. Therefore, if a Responsible Party holds for example, the identity number of a person, that person will be identifiable and qualify as a Data Subject in terms of POPIA, since their identity number can be used to distinguish them from other persons.

6.3.1.7. Data Subjects are not only South African citizens or persons domiciled in South Africa. A Data Subject can therefore be resident anywhere in the world, with the Processing of their Personal Information by a local Responsible Party also qualifying the person as a Data Subject.

6.3.2. *The Responsible Party*

6.3.2.1. POPIA describes a Responsible Party as the party responsible for ensuring compliance with the Act when Processing Personal Information, and encompasses any public or private bodies or any other person that either alone or together with others, determines the purpose of and means for Processing Personal Information.

6.3.2.2. Therefore, a Responsible Party is the entity (the 'who') that requires the Personal Information of a Data Subject for a particular purpose (the 'why') and consequently establishes how such Personal Information will be Processed to achieve its goals (the 'how').

6.3.2.3. A Responsible Party will be held accountable and be liable to face the consequences of non-compliance if the provisions of POPIA are not complied with.

6.3.2.4. A Responsible Party will request a Data Subject to provide their Personal Information, for example their name, identity number, banking details and residential address by way of a client information form, in order to achieve some purpose as determined by the Responsible Party.

6.3.2.5. The purpose behind the Processing of Personal Information will vary from Responsible Party to Responsible Party. This will depend on the business of the Responsible Party and why they need certain Personal Information of Data Subjects.

6.3.2.6. In the event that Personal Information is collected by a business and thereafter transferred to another party for further Processing, such as the storage, use for a particular purpose or destruction, the first business will qualify as the Responsible Party in terms of POPIA.

6.3.2.7. It is important to remember that persons who Process Personal Information purely for a household or personal reason will not qualify as Responsible Parties in terms of POPIA. For example, the collection and storage of names and contact numbers of family and friends will not attract POPIA compliance, since the risk to the right to privacy of third parties is minimal.

6.3.3. *The Operator*

6.3.3.1. POPIA allows Responsible Parties to outsource Personal Information to other parties for further Processing. These third parties that will be responsible for the further Processing of Personal Information are known as Operators.

6.3.3.2. An Operator is described by POPIA as any person or entity that Processes Personal Information on behalf of a Responsible Party in terms of a contract or mandate, without falling under the direct authority of the Responsible Party.

6.3.3.3. Operators often include businesses such as data centres that store Personal Information on behalf of a Responsible Party, call centres that conduct direct marketing activities for Responsible Parties and research centres that Process and analyse data on behalf of Responsible Parties who require such information for a particular purpose.

6.3.3.4. The test to determine whether or not an entity can be classified as an Operator involves two questions:

6.3.3.4.1. Do they determine the purpose ("*why*") and means ("*how*") for the Processing of the Personal Information?

6.3.3.4.2. Do they Process the Personal Information on the instruction of a Responsible Party in accordance with some mandate or agreement?

6.3.3.5. If the first question is answered "no" and the second question "yes", then the entity will qualify as an Operator in terms of POPIA.

6.3.3.6. If the first question is answered "yes", then the entity will not be considered as an Operator in terms of POPIA and it will not be necessary to ask the second question, since it will fall outside the definition.

6.3.3.7. If the second question is answered "no" under any circumstance, then the entity will also not be considered as an Operator in terms of POPIA, as it will fall outside the scope of the definition.

6.3.3.8. It is important to keep in mind that a business entity or institution may qualify as both a Responsible Party and an Operator in different circumstances.

6.3.4. *The Information Officer*

6.3.4.1. POPIA requires that Responsible Parties put forward an individual who will be responsible, within that entity or institution, for ensuring compliance with POPIA and being responsible for the governance, management and security of Personal Information. These persons are known as Information Officers.

6.3.4.2. POPIA emphasises and expands on the role of Information Officer, as established and defined in the Promotion of Access to Information Act 2 of 2000 ("**PAIA**"). Information Officers are relevant in relation to both public and private bodies.

6.3.4.3. The Information Officer of a Responsible Party will generally be the executive head of that entity or institution, as well as any person duly appointed by the Information Officer to perform his or her duties. Such appointed person is known as a deputy Information Officer.

6.3.4.4. Employees will be informed from time to time who the Information Officer and deputy Information Officer(s) of the Company are. All queries and concerns regarding POPIA, our compliance obligations and this Policy should be directed to the deputy Information Officer.

6.3.5. *The Information Regulator*

6.3.5.1. POPIA provides for the establishment of the Information Regulator. This statutory body is responsible for the enforcement and implementation of POPIA.

6.3.5.2. The Information Regulator has been bestowed with extensive powers in terms of POPIA, including the power to receive and investigate complaints, impose sanctions and publish guidelines and guidance documents in terms of POPIA.

6.3.5.3. Practically speaking, the Information Regulator is the watchdog that ensures that POPIA is correctly adhered to by Responsible Parties and to set the standards that need to be met for compliance with the Act.

6.4. **Additional considerations**

6.4.1. *Direct marketing activities*

Direct marketing is considered to be a legitimate business interest globally and in South Africa. POPIA imposes certain rules in relation to direct electronic marketing practices.

6.4.2. *Transfer of Personal Information across borders*

6.4.2.1. Personal Information may be transferred to various countries worldwide by a variety of different means. These means may include (but are not limited to) transfers by post, telecommunications systems, satellite computer networks and even personal delivery of data.

6.4.2.2. The increasing use of the internet, electronic mail and cloud-based systems and storage has especially facilitated the convenience and expedience with which information can be transferred from one country to another.

6.4.2.3. At its core, the transfer of Personal Information to foreign countries should not be viewed as a separate issue from the transfer of Personal Information within South Africa. It merely constitutes a more complex form of transfer since it is complicated by various considerations such as sovereignty and trade. Ultimately, a Data Subject's Personal Information should not receive a lower standard of protection in a foreign country than it would have received if the provisions of POPIA continued to apply to the Processing of such information.

6.4.2.4. In circumstances where Personal Information is transferred outside South Africa, the Responsible Party must notify all Data Subjects that it intends to transfer their Personal Information to another country and inform the Data Subjects of the level of protection that their information will have in such third-party country. This is particularly relevant where use is made of cloud storage or data is shared by a company with branches or partners in other countries.

6.4.2.5. These considerations are based on the underlying intention of POPIA that Personal Information should remain protected and secure even after it has been transferred to another country where POPIA does not apply.

6.4.2.6. The most effective way to ensure that a cross border transfer of Personal Information is POPIA compliant, is to obtain the consent of the relevant Data Subject(s) whose Personal Information is being transferred abroad.

6.4.2.7. In light of the international move towards information and data protection, there are many jurisdictions worldwide that afford the same, similar or higher standards of protection to the processing of personal information. The European Union and the United Kingdom are primary among these.

6.5. **The conditions for lawful Processing**

6.5.1. POPIA makes provision for eight conditions, or pillars, which govern the lawful Processing of Personal Information.

6.5.2. As a Responsible Party, these so-called pillars of compliance must be adhered to by the Company in order to ensure that we successfully discharge our obligations in terms of POPIA and lawfully Process Personal Information. Our approach to ensuring compliance with our obligations under each condition is set out more comprehensively below.

6.5.3. *Condition 1: Accountability*

6.5.3.1. The Company carries the obligation of ensuring that Personal Information is Processed lawfully and that the conditions to ensure such lawful Processing are complied with. POPIA makes the Company accountable for its Processing activities and sets out our liability in the event that Personal Information is not Processed in a lawful manner.

6.5.3.2. It is important to keep in mind that the Company remains accountable even if the Processing of Personal Information is outsourced, or if Personal Information is shared with third parties. Such sharing of Personal Information outside the Company must therefore be carefully scrutinised and only take place in accordance with the provisions of POPIA and this Policy.

6.5.4. *Condition 2: Processing limitation*

6.5.4.1. The Processing Limitation condition entails that the Company -

6.5.4.1.1. should only allow minimal Processing of Personal Information;

6.5.4.1.2. should obtain the consent of Data Subjects in order to Process Personal Information;

6.5.4.1.3. must be justified in Processing the Personal Information; and

6.5.4.1.4. should as far as is reasonably practicable, collect Personal Information directly from the particular Data Subject.

6.5.4.2. Personal Information may only be Processed if such Processing is adequate, relevant and not excessive. Accordingly, the nature and scope of the Processing activity must be clear and Employees should at all times be mindful of Personal Information being Processed and ensure that same is relevant for its purpose and not more than is necessary to achieve such purpose.

6.5.5. *Condition 3: Purpose specification*

6.5.5.1. POPIA requires that Personal Information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the Company.

6.5.5.2. Data Subjects should also be informed of such Processing and the purpose thereof.

6.5.6. *Condition 4: Further Processing limitation*

6.5.6.1. Any further Processing of Personal Information must be in accordance or compatible with the purpose for which the Personal Information was originally collected.

6.5.6.2. This original purpose must not be deviated from during the course of the Processing of Personal Information.

6.5.6.3. If the Personal Information collected will be used for any purpose other than the original purpose, the relevant Employee must first obtain consent from the Data Subject prior to such Processing, or such Processing must otherwise be justified.

6.5.7. *Condition 5: Information quality*

6.5.7.1. Data quality is a significant aspect to be considered since data that is of a sub-standard quality may negatively affect a Data Subject. Data quality is also important when it is considered that Personal Information generally carries commercial value.

6.5.7.2. The Employee responsible for collecting/Processing the Personal Information must ensure that the information is up to standard, and where applicable up to date where such information is outdated.

6.5.7.3. POPIA obliges the Company to take reasonable practicable steps to ensure that all the Personal Information which we collect is complete, accurate and not misleading.

6.5.8. *Condition 6: Openness*

6.5.8.1. A cornerstone of POPIA is the promotion of transparency. This goal is advanced through the condition of "openness" which, in essence, requires that Data Subjects must be notified when their Personal Information is being Processed.

6.5.8.2. Simply put, this means that information should not be Processed in secret. To this end, the Employee handling the Processing of the Personal Information must follow the internal procedures, set out in the Compliance Framework to ensure that the Data Subject is aware that their Personal Information is being Processed by the Company.

6.5.8.3. Records must also be kept all employees of all Processing activities conducted by them in relation to a particular Data Subject.

6.5.9. *Condition 7: Security safeguards*

6.5.9.1. The use of the word "protection" in the title of POPIA places emphasis on securing Personal Information and an obligation to ensure that it remains safe. Ensuring the security of Personal Information of Data Subjects is the most important condition for lawful Processing in terms of POPIA, since security failures and breaches have the potential for Data Subjects to suffer significant harm.

6.5.9.2. The harm that is suffered by Data Subjects is also high risk for the Company, as any breaches in data security damages the name of the Company. The security policy, attached as "**Annexure C**" (*Safety and Security Protocols*) hereto must be adhered to by all Employees Processing Personal Information.

6.5.9.3. POPIA obliges the Company to ensure the integrity and confidentiality of Personal Information in our possession. Data security is advanced by appropriate and reasonable technical and organisational measures as set out in the Compliance Framework to prevent the loss of, damage to, unauthorised destruction of, unlawful access to or the unlawful Processing of Personal Information.

6.5.9.4. In advancing data protection, the Company must take into account generally accepted information security practices and procedures that it may put in place, as well as practices and procedures that may be required by it in terms of industry specific rules and regulations. These will be communicated by Senior Management to Employees from time to time, under the auspices of this Policy and as changing circumstances and developments may require. Employees must at all times be up to date and aware of these requirements and must regularly confirm that their knowledge in this regard is up to date.

6.5.10. *Condition 8: Data Subject participation*

6.5.10.1. Data Subjects are entitled, in terms of POPIA, to request access to the Personal Information held by the Company, as well as the amendment and deletion of such information.

6.5.10.2. The Company is obliged, if so requested, to provide confirmation to Data Subjects that we hold their Personal Information (free of charge), to provide a description of the Personal Information in question

and to confirm the identity of all third parties or the categories of third parties who have received their Personal Information. The procedures for submitting such a request to the Company are contained in the PAIA Manual of the Company, which is available on the website of the Company at: www.umbhaba.co.za

7. COMPLIANCE FRAMEWORK

PILLARS	COMPLIANCE DUTY	APPLICABLE SECTIONS OF CHAPTER 3 OF POPIA
1	Accountability	8
2	Processing limitation	9, 10, 11, 12
3	Purpose specification	13, 14
4	Further Processing limitation	15
5	Information quality	16
6	Openness	17, 18
7	Security safeguards	19, 20, 21, 22
8	Data Subject participation	23, 24, 25

7.1. PILLAR 1: Ensuring accountability, both internally and when outsourcing the Processing of Personal Information

7.1.1. *Internal Accountability*

7.1.1.1. The Company endorses a policy of responsibility, not only by the Company to Data Subjects but also by Employees to the Company.

7.1.1.2. Employees must keep in mind that the Company is accountable in terms of POPIA when we Process any Personal Information as a Responsible Party. Therefore care should always be taken by all Employees when dealing with Personal Information.

7.1.1.3. In the event that any Employee is uncertain of our POPIA obligations when dealing with Personal Information internally, same should be discussed with the Information Officer without delay.

7.1.2. *Accountability when outsourcing Processing of Personal Information*

7.1.2.1. In order to ensure that the principle of accountability is adhered to, the following measures will be taken when Operators Process Personal Information on behalf of the Company:

7.1.2.1.1. All contracts with Operators should include clauses which require the Operator to make use of security safeguards that measure up to or surpass the standards used by the Company and those required in terms of POPIA.

7.1.2.1.2. Provision should be made in all Operator agreements for the Operator to be held liable for damages suffered if a claim for a Data Breach is successful against the Company.

7.1.2.2. In the event that any Employee is uncertain of our POPIA obligations when outsourcing Personal Information to Operators or otherwise sharing of Personal Information outside the Company, same should be discussed with the Information Officer without delay.

7.2. PILLAR 2: Limiting the Processing of Personal Information

7.2.1. *Lawful Processing*

7.2.1.1. All Personal Information Processed by Employees must be Processed in a manner that is lawful, reasonable and does not infringe on the privacy of the Data Subject.

7.2.1.2. As a general rule, all Personal Information Processed by Employees must be treated as sensitive information and must not be disseminated or discussed with parties not involved in the Processing. More comprehensive detail relating to which Employees are permitted to have access to which type of information is set out in "**Annexure A**" (*Employee access to Information*) hereto.

7.2.2. *Minimality*

7.2.2.1. Before Processing Personal Information, the Employee should consider the following:

7.2.2.1.1. Is the Personal Information adequate for the purpose for which it is being Processed?

7.2.2.1.2. Is the Personal Information relevant for the purpose for which it is being Processed?

7.2.2.1.3. The Personal Information which is being Processed should not be excessive, in other words, only the necessary and required Personal Information should be Processed to achieve the goal for which it is Processed.

7.2.2.2. If the answer to any of the above considerations is in the negative, the Personal Information to be Processed should be reconsidered and revised to ensure conformity with this Policy, and in the event that any doubts persist, these should be brought to the attention of and discussed with the Information Officer without delay.

7.2.3. *Consent, justification and objection*

7.2.3.1. Processing Personal Information should only commence once consent is received from the Data Subject

to Process their information, where the Data Subject is a minor, a competent person should consent on their behalf.

7.2.3.2. The consent of the Data Subject is not required in the following circumstances:

7.2.3.2.1. when the Processing occurs in the process of carrying out obligations in terms of a contract to which the Data Subject is a party;

7.2.3.2.2. when the Processing is conducted by the Company to meet a statutory obligation;

7.2.3.2.3. where the Processing protects a legitimate interest of the Data Subject; or

7.2.3.2.4. when Processing is necessary to pursue the interests of the Company or a third party to whom the Personal Information is supplied.

7.2.3.3. Adequate records should be kept by the Employee who obtained consent from the Data Subject to prove that consent for the Processing was indeed obtained. These records should be stored in hard copy on the physical file (if applicable) and an electronic version on the electronic platforms used by the Company.

7.2.3.4. While practical measures to prove consent may vary from time to time, the signed client mandate received from clients is sufficient consent to Process their Personal Information in line with their instructions.

7.2.4. *Collection directly from Data Subject*

7.2.4.1. As a point of departure, Personal Information should always be collected directly from the Data Subject as far as possible. The following circumstances are exceptions to this rule:

7.2.4.1.1. The Personal Information is available in or collected from a public record or has been deliberately been made public by the Data Subject.

7.2.4.1.2. Either the Data Subject or a competent person on behalf of the Data Subject has consented to the collection of their Personal Information from another source.

7.2.4.1.3. The legitimate interests of the Data Subject would not be prejudiced by collection from another source.

7.2.4.1.4. When collection from another source is necessary -

7.2.4.1.4.1. for the Company to meet a statutory obligation;

7.2.4.1.4.2. to maintain the legitimate interests of the Company or a third party to whom the Personal Information is supplied; and

7.2.4.1.4.3. for use in court or tribunal proceedings (such as arbitration) that have either already commenced or are reasonably being contemplated.

7.2.4.1.5. The lawful purpose of collecting the Personal Information would be prejudiced by collecting directly from the Data Subject.

7.2.4.1.6. Collection directly from the Data Subject is not reasonably practicable in any particular case.

7.2.4.2. Where collection from any source other than the Data Subject directly is contemplated, such collection should be approved by the relevant Employee in writing, to be kept on record, setting out why collection from the Data Subject was not appropriate in the particular circumstances. In the event that an Employee has any uncertainty regarding the collection of any information from a source other than the Data Subject, this should be brought to the attention of and discussed with the Information Officer without delay.

7.3. **PILLAR 3: Processing Personal Information in line with its purpose**

7.3.1. *Collection for specific purpose*

7.3.1.1. Any Personal Information collected must be collected for a specific purpose and be related to a function or activity that is performed by the Company. This will substantially differ from case to case, however the provisions of this Policy and relevant legislation should be used as guide to determine to what extent Personal Information is necessary to achieve the desired outcome for any matter.

7.3.1.2. The Data Subject should therefore be informed of what the purpose for the Processing of their Personal Information is.

7.3.2. *Retention and restriction of records*

7.3.2.1. POPIA requires that once the purpose for which the Personal Information was collected has been achieved, it should no longer be retained. Though this is a general requirement, the nature of the work that the Company engages in means that retention of records for varying periods of time remains essential. The following circumstances are exceptions that apply to such records and Personal Information, records may be retained if -

7.3.2.1.1. retention is required by law;

7.3.2.1.2. the Company requires the record for lawful purposes related to its functions and activities;

7.3.2.1.3. retention is agreed to in a contract between the Company and the Data Subject; or

7.3.2.1.4. where consent for such retention has been obtained from either the Data Subject or a competent person, in the case of a minor.

7.3.2.2. Where the Company has made use of the Personal Information to make a decision of the Data Subject -

7.3.2.2.1. the record must be retained as required by law or any applicable code of conduct; or

7.3.2.2.2. if such law or code of conduct is not applicable, records should be retained for a period sufficient to allow the Data Subject a reasonable opportunity to request access to the records in line with the POPIA compliant PAIA Manual.

7.3.2.3. Within a period of 12 (TWELVE) months after the circumstances contemplated in paragraphs 7.3.2.1 and 7.3.2.2 above cease to exist, the records should be destroyed or deleted.

7.3.2.4. The destruction or deletion contemplated in paragraph 7.3.2.3 should render the records unidentifiable and incapable or reconstruction.

7.3.2.5. The Processing of Personal Information by the Company will be restricted if -

7.3.2.5.1. the accuracy of the Personal Information is contested by the Data Subject, this restriction will be applicable until the Company can verify the accuracy of the Personal Information;

7.3.2.5.2. the Company has achieved the purpose for which the Personal Information was initially collected and it is now merely retained for record keeping purposes;

7.3.2.5.3. the Processing took place in an unlawful manner. However, the Data Subject may request that the Personal Information not be deleted or destroyed and that its Processing be restricted instead; or

7.3.2.5.4. the Data Subject requests that the Personal Information be transferred to an alternative automated processing system.

7.3.2.6. The Personal Information identified in paragraph 7.3.2.5 may only be stored and not Processed further, unless it is Processed for -

7.3.2.6.1. purposes of proving any legitimate matter related to the initial purpose of the Processing by the Company;

7.3.2.6.2. a matter where consent for such Processing has been obtained from either the Data Subject or a competent person, in the case of a minor;

7.3.2.6.3. purposes of protecting the interests of another natural or legal person; or

7.3.2.6.4. the benefit of the public interest.

7.3.2.7. If the Processing of Personal Information is restricted in terms of paragraph 7.3.2.5, the Data Subject must be informed prior to the lifting of the restriction of the Processing of such information.

7.3.3. In the event that an Employee has any uncertainty regarding purpose of the Processing of the Personal Information, this should be brought to the attention of and discussed with the Information Officer without delay.

7.4. **PILLAR 4: Further Processing to be done in line with its original purpose**

7.4.1. Any further Processing of Personal Information in the possession of the Company must be Processed in accordance or compatible with the purpose for which it was originally collected. The further Processing of Personal Information should take into account -

7.4.1.1. the relationship between the purpose of the intended further Processing and the purpose for which the information was originally collected;

7.4.1.2. the nature of the Personal Information concerned;

7.4.1.3. the consequences, if any for the Data Subject due to the further Processing;

7.4.1.4. the manner that the Personal Information was initially collected; and

7.4.1.5. any contractual obligations and rights between the Data Subject and the Company.

7.4.2. The further Processing is compatible with the original purpose if -

7.4.2.1. consent for such Processing has been obtained from either the Data Subject or a competent person, in the case of a minor;

7.4.2.2. the Personal Information is available in or collected from a public record or has been deliberately been made public by the Data Subject; and/or

7.4.2.3. the further Processing is needed for -

7.4.2.3.1. compliance with any statutory duty; and

7.4.2.3.2. for use in court or tribunal proceedings that have either already commenced or are reasonably being contemplated;

7.4.3. The further Processing of Personal Information may also take place under such exceptions as published by the Information Regulator from time to time pursuant to section 37 of POPIA.

7.4.4. In the event that an Employee has any uncertainty regarding whether further processing of the Personal Information is in line with its original purpose, this should be brought to the attention of and discussed with the Information Officer without delay.

7.5. **PILLAR 5: Ensuring the quality of Personal Information**

7.5.1. POPIA places a duty on the Company to put in place reasonably practicable measures that Personal Information Processed by the company is complete, accurate and updated where necessary. To this end, the following is expected of Employees:

7.5.1.1. Where any matter, relationship or transaction continues over a period of time exceeding 12 (TWELVE) months, the Data Subject should be contacted to confirm the continued accuracy and comprehensive nature of information in possession of the Company.

7.5.1.2. Should the responsible Employee have any reason to reasonably suspect that the information in possession of the Company is incorrect or outdated, the Employee must contact the Data Subject to ascertain the accuracy of the Personal Information.

7.5.1.3. The purpose of the Personal Information in possession of the Company should be taken into consideration when considering the above, if a particular matter requires more frequent confirmation of such information, the Employee should undertake such follow ups with due care and as often as may be necessary in the circumstances.

7.5.2. In the event that an Employee has any uncertainty regarding data quality and their obligations in this regard, this should be brought to the attention of and discussed with the Information Officer without delay.

7.6. **PILLAR 6: Ensuring transparency and openness**

7.6.1. **Documentation**

POPIA requires that the Company retain documentation to prove the Processing of all Personal Information that the Company Processes. These records must be stored in electronic and where applicable, physical files relating to the relationship between the Company and the Data Subject involved, where applicable.

7.6.2. **Notification to Data Subject when collecting Personal Information**

7.6.2.1. The following practical measures are to be put in place to ensure that Data Subjects are informed that the Company is Processing their Personal Information, to the extent that such Processing is not otherwise justified in terms of POPIA and notification is not required (these circumstances are depicted in paragraph 7.6.2.2 below):

7.6.2.1.1. An electronic mail should be transmitted to the Data Subject, indicating that the Company is Processing their Personal Information and should include a link or document indicating the following-

7.6.2.1.1.1. the Personal Information being collected and where the information is not collected from the Data Subject, the source from which it is collected;

7.6.2.1.1.2. the name and address of the Company;

7.6.2.1.1.3. the purpose for which the Personal Information is being collected;

7.6.2.1.1.4. whether the supply of the Personal Information by that data subject is voluntary or mandatory;

7.6.2.1.1.5. the consequences of failure to provide the Personal Information;

7.6.2.1.1.6. any particular law authorising or requiring the collection of the Personal Information, such as, for example, the Financial Intelligence Centre Act 38 of 2001;

7.6.2.1.1.7. if applicable, that the Company intends to transfer the Personal Information to a third country or international organisation and the level of protection afforded to the information by that third country or international organisation;

7.6.2.1.1.8. any further relevant information, such as the—

7.6.2.1.1.8.1. recipient or category of recipients of the Personal Information;

7.6.2.1.1.8.2. nature or category of the Personal Information;

7.6.2.1.1.8.3. existence of the right of access to and the right to rectify the Personal Information collected;

7.6.2.1.1.8.4. existence of the right to object to the Processing of Personal Information; and

7.6.2.1.1.8.5. right to lodge a complaint to the Information Regulator and the contact details of the Information Regulator, which is necessary, having regard to the specific circumstances in which the Personal Information is or is not to be Processed, to enable Processing in respect of the Data Subject to be reasonable.

7.6.2.1.2. The electronic mail should be transmitted to the Data Subject prior to collection of Personal Information from the Data Subject, this is not required where the Data Subject is already aware of the information set out in paragraph 7.6.2.1.1, such as for example to existing customers who already are aware that the Company is Processing their Personal Information and have been notified of all relevant information, or if the Processing of Personal Information is otherwise justified in terms of POPIA (these circumstances are depicted in paragraph 7.6.2.2 below).

7.6.2.1.3. In any matter where the collection does not take place directly from the Data Subject, the Data Subject should be notified prior to the collection of their Personal Information and where this is not reasonably practicable, as soon as possible thereafter, provided that the Processing of Personal Information is otherwise justified in terms of POPIA (these circumstances are depicted in paragraph 7.6.2.2 below).

7.6.2.2. Notification as set out in paragraph 7.6.2.1 is not necessary if:

7.6.2.2.1. the Data Subject or competent person, in the case of a minor, has consented to and indicated that such notification is not required;

7.6.2.2.2. non-compliance will not negatively prejudice the legitimate interests of the Data Subject as set out in POPIA and this Policy;

7.6.2.2.3. the notification is prevented by any legislation;

7.6.2.2.4. the Personal Information collected is for use in court or tribunal proceedings that have either already commenced or are reasonably being contemplated;

7.6.2.2.5. compliance would prejudice a lawful purpose of the collection;

7.6.2.2.6. the circumstances of a particular matter render such notification reasonably impracticable; or

7.6.2.2.7. the information collected will be used in such a way that the Data Subject cannot be identified or will be used for historical, statistical or research purposes.

7.6.2.3. In circumstances where an Employee has any uncertainty pertaining to the notification requirements of the Company, same should be discussed with the Information Officer.

7.6.3. **Privacy Policy**

It should also be kept in mind that the Privacy Policy of the Company also assists with its notification requirements in terms of POPIA, and essentially sets out our commitment to privacy and upholding the provisions of POPIA. Our privacy policy may be accessed at our company's intranet.

7.7. **PILLAR 7: Ensuring the implementation of security safeguards**

7.7.1. *Security measures on integrity and confidentiality of Personal Information*

7.7.1.1. In order to ensure that all Personal Information Processed by the Company is kept secure, Personal Information must be Processed and particular focus is placed on the storage in compliance with the appropriate security measures as set out in "**Annexure C**" (*Safety and Security Protocols*) and "**Annexure D**" (*Password Policy*).

7.7.1.2. With the aim of strengthening compliance with the provisions of POPIA, annual audits will be conducted to ensure that the security measures as set out in "**Annexure C**" (*Safety and Security Protocols*) and "**Annexure D**" (*Password Policy*) are up to industry standards. The audit should include investigations into possible risk for security breaches, and solutions for such risks should be presented to the Information Officer of the Company who will then present the proposals to the Senior Management of the Company for implementation.

7.7.2. *Information processed by an Operator or person acting under authority*

Where an Operator Processes Personal Information on behalf of the Company, the following provisions must be included in any agreement to conduct such Processing:

7.7.2.1. the Operator must inform the Company when Processing of such Personal Information occurs; and

7.7.2.2. measures should be included in all agreements to conduct such Processing to safeguard the confidentiality of such Personal Information.

7.7.3. *Security measures regarding Personal Information processed by Operator*

7.7.3.1. All contracts with Operators should include clauses which require the Operator to make use of security safeguards that measure up to or surpass the standards used by the Company.

7.7.3.2. The Operator should be required in terms of such agreement to notify the Company immediately where there are reasonable grounds to believe that the Personal Information of a Data Subject has been accessed or acquired by any unauthorised person.

7.7.3.3. Provision should be made in all operator agreements for the Operator to be held liable for damages suffered if a claim for a Data Breach is successful against the Company.

7.7.4. *Notification of security compromises*

Notification in the event of a Data Breach is mandated by POPIA, the specifics of the internal procedure to follow in the case of a Data Breach is set out in "**Annexure B**" (*Data Breach Plan*).

7.8. **PILLAR 8: Enabling Data Subject participation**

7.8.1. *Access to personal information*

Section 23 of the Act requires that procedures be put in place by the Company to enable Data Subjects who have provided adequate proof of identity to request access to their Personal Information. The Company has put in place a POPIA Compliant PAIA Manual, which can be accessed at www.umbhaba.co.za which sets out the relevant procedures for such requests.

7.8.2. *Correction of personal information*

Section 24 of the Act requires that procedures be put in place by the Company to enable Data Subjects who have provided adequate proof of identity to request the correction or amendment of their Personal Information, which is in the possession of the Company. The Company has put in place a POPIA Compliant PAIA Manual, which can be accessed at www.umbhaba.co.za which sets out the relevant procedures for such requests.

7.8.3. *Manner of access*

Section 25 of the Act requires that the Company put in place a POPIA Compliant PAIA Manual, the Company has done so, and this can be accessed at www.umbhaba.co.za which sets out the relevant procedures for such requests.

8. MONITORING OF COMPLIANCE

8.1. The Information Officer is authorised in terms of this Policy to, from time to time, conduct internal audits and compliance assessments across all business areas of the Company, in order to -

8.1.1. establish the compliance status of the Company in terms of the Act;

8.1.2. adherence by Employees to this Policy;

8.1.3. confirm adequate recordkeeping of Personal Information documentation by the Company; and

8.1.4. identify training and support needs of Employees in respect of this Policy.

8.2. Such audit and compliance assessments reports will be submitted to Senior Management for consideration and attention, and must include suggested remedial measures by the Company for the correction of any identified compliance shortfalls or gaps and recommendations for the improvement of the Compliance Framework of the Company.

9. BREACH OF THIS POLICY

Subject to paragraph 10.4 below, any Employee that fails to comply with this Policy may be subject to disciplinary action as a result of such failure.

10. EMPLOYEE RESPONSIBILITIES

10.1. All our Employees are responsible for ensuring that they read and understand this Policy. In addition, compliance with this Policy and its contents are expected of all our Employees.

10.2. All Employees under our control are equally responsible for the Processing of Personal Information in line with this Policy and are required to avoid any and all activities that could lead to, or imply, a breach of this Policy.

10.3. The duty of Employees to report suspicious activities includes the duty to report if they have a reasonable suspicion that a Data Breach may have occurred, is in the process of occurring, or may occur in future.

10.4. Failure to comply with this Policy will lead to disciplinary action up to and including dismissal depending on the severity of the actions of the employee.

11. INTERNAL PROCEDURES TO RAISE CONCERNS

11.1. The internal procedures to raise concerns are not set out in detail in this Policy, however any employee who wishes to raise a concern should first contact their line manager and inform them of the circumstances.

11.2. Should the line manager fail to take action or fail to take appropriate action, the employee may approach the Information Officer for this Policy directly to raise their concern in a more formal manner.

11.3. Any person or employee who does raise such a concern shall not be identified to fellow employees and shall be afforded all reasonable protection of their privacy to prevent problems in the workplace.

12. TRAINING AND COMMUNICATION

12.1. As part of the induction process for new employees, they will be required to attend training in relation to this Policy to ensure that no employee is uninformed of the contents of this Policy.

12.2. Where an employee performs work in different jurisdictions, the employee is expected to comply with the requirements of the respective jurisdictions which laws are applicable at any given moment in time.

13. RISK ASSESSMENT, MONITORING AND REVIEW

13.1. We recognise that as time passes changes may become necessary to ensure that this Policy remains effective and up to date. The Senior Management of the Company, together with the Information Officer, will on an annual basis conduct an audit/review of this Policy and its efficacy to ensure that high standards are maintained at all times in relation to our commitment to protecting Personal Information.

13.2. Should any need for improvements or adjustments arise, they will be implemented as soon as is reasonably possible and has been approved by the Senior Management of the Company.

ANNEXURE A: EMPLOYEE ACCESS TO INFORMATION

For the purposes of the Processing of Personal Information within the Company, there are generally 3 (THREE) categories, namely information relating to clients; Employees and service providers.

1. CLIENTS

1.1. The Personal Information of all clients should be treated as confidential and should be Processed in compliance with the provisions of this Policy by all Employees.

1.2. Any queries relating to the Processing of clients' Personal Information should be directed to the Information Officer.

2. EMPLOYEES

2.1. The Personal Information of all Employees shall be treated as confidential, and should be Processed in compliance with the provisions of this Policy by all Employees.

2.2. Access to the Personal Information of fellow Employees, except as is generally available and known to Employees in the course and scope of their employment, is generally not permitted, and any queries in this regard should be directed to the Human Resources Manager of the Company; the finance department or Senior Management.

3. SERVICE PROVIDERS

3.1. The Personal Information of all service providers shall be treated as confidential, and should be Processed in compliance with the provisions of this Policy by all Employees.

3.2. Any queries in this regard should be addressed to the Information Officer.

ANNEXURE B: DATA BREACH PLAN

In line with the provisions of POPIA, the Company has formulated and follows the provisions of a Data Breach Plan, which will be provided and is accessible to all Employees. This plan will be updated from time to time and it is the responsibility of all Employees to ensure that they are familiar with the provisions of this plan and their responsibilities in this regard. Any queries or concerns regarding this plan should be addressed to the Information Officer.

ANNEXURE C: DATA SECURITY PROTOCOLS

This Annexure sets out the Data Security Protocols that the Company implements to ensure that Personal Information is Processed in compliance with the provisions of POPIA and that all Personal Information in possession of the Company is kept secure.

1. The Company shall implement Technical and Organisational Security Measures appropriate to protect the Personal Information against loss of, damage to or unauthorised destruction and unlawful access to such Personal Information, and against all other unlawful forms of Processing of the Personal Information, and shall ensure that these measures ensure a level of security appropriate to the risks presented by the Processing and the nature of the Personal Information to be protected having due regard to generally accepted information security practices and procedures which may apply to the Company generally or be required in terms of specific industry or professional rules and regulations, which shall include reasonable measures to –

1.1. identify all reasonably foreseeable internal and external risks to Personal Information in its possession or under its control;

1.2. establish and maintain appropriate safeguards against the risks identified;

1.3. regularly verify that the safeguards are effectively implemented; and

1.4. ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

2. Any person acting under the authority of the Company, as well as the Company itself, will comply with the security measures enacted or to be enacted by the relevant data protection authorities or as provided by law, as the case may arise, including but not limited to, the guidelines published by the Information Regulator.

ANNEXURE D: PASSWORD POLICY

In line with the provisions of POPIA, the Company has formulated and follows the provisions of the following password policy:

Objective

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of our company's entire corporate network. As such, all our company's employees (including contractors and vendors with access to our company's systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

This policy establishes a standard for the creation of strong passwords, the protection of those passwords and the frequency of change.

Scope

The scope of this policy includes all employees who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any our company's facility, who have access to our company's network, or who store any non-public information of our company.

User Authentication

Every user must be assigned a unique user account (user ID) and a password for access to our company's systems. Shared or group user IDs are prohibited for user-level access. Systems and applications must authenticate using a password or token entry. The use of non-authenticated user IDs (i.e., those without passwords) or user IDs not associated with a single identified user are prohibited. The account will lock a user out after six invalid login attempts within 30 minutes. Locked accounts shall remain locked for at least 30 minutes or until the System Administrator unlocks the account. Users may contact the IT Service Desk to have their account unlocked. Multifactor authentication is required for all users accessing our company's systems remotely.

Password Management

Passwords must be created and managed in accordance with this section.

Password Requirements

- All user-level of our company's network passwords will expire every 90 days and must be changed.
- New passwords cannot be the same as the previous four passwords.
- Passwords must be at least eight characters in length. Longer is better.
- Passwords must contain both uppercase and lowercase characters (e.g., a-z and A-Z).

- Passwords must contain at least one number (e.g., 0-9).
- Accounts shall be locked after six failed login attempts within 30 minutes and shall remain locked for at least 30 minutes or until the System Administrator unlocks the account.

To unlock an account or change a password without logging in, some of our company's systems require the Technology Department to provide a new temporary password to the user. In such cases, passwords must be provided verbally and the user must immediately log in and change the account password.

Passwords should not be shared with anyone, including IT support personnel, unless approved by the IT Security Specialist.

All passwords are to be treated as sensitive, confidential information. If someone requests your password(s), please inform him or her that you cannot provide that information per our company's policy and contact the IT Security Specialist about the request. If you suspect an account or password has been compromised, report the incident immediately and change all related passwords.

The Technology Department or authorized outside "penetration testers" may perform password cracking or guessing on a periodic or random basis to test the security of our company's network. If a password is guessed or cracked during one of these scans, the user will be required to change it. Password cracking and guessing are not to be performed by anyone outside of the Technology Department or an approved third-party auditor.

The Technology Department strongly encourages the use of a password manager program to help ensure that all passwords are strong, unique and easily changed. Users should open an IT Service Desk ticket with a request for more information on password managers allowed on our company's network and for assistance in getting the password manager installed and configured on their computer.

Guidelines for Password Construction

A strong password:

- Contains both uppercase and lowercase characters (e.g., a-z and A-Z).
- Contains digits and punctuation characters (e.g., 0-9 and !@#$%^&*).
- Is at least 8-15 alphanumeric characters long and is a passphrase (e.g., "Ohmy1stubbedmyt0e").
- Is not a single word in any language, slang, dialect or jargon (e.g., "password" or "Fluffy").
- Is not based on personal information, names of family members, etc.

Passwords should never be written down or stored online. Employees should try to create passwords that can be easily remembered. One way to do this is to create a password based on a song title, affirmation or other phrase. For example,

the phrase might be "This may be one way to remember," and the password could be "TmB1w2R!" or "Tmb1W>r~" or some other variation.

Use of Passwords and Passphrases for Remote Access Users

Access to our company's network via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

Passphrases

Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all and the private key that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of uppercase and lowercase letters as well as numeric and punctuation characters. An example of a good passphrase is "Vaca@The#OBX!$MyDreamin!"

All of the rules above that apply to passwords apply to passphrases.

Enforcement

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

This policy will be updated from time to time and it is the responsibility of all Employees to ensure that they are familiar with the provisions of this policy and their responsibilities in this regard. Any queries or concerns regarding this policy should be addressed to the Information Officer.