IFSA (PTY) LTD – 2000/005153/07

MANDATORY ITEMS – POLICIES

ITEM NO. 2.1 – POLICY ON LAWFUL PROCESSING OF PERSONAL INFORMATION

1. DEFINITIONS

1.1. Unless the context clearly indicates a different intention, expressions defined in the Act will bear the same meanings herein. For ease of reference, the following prevalent definitions recorded in the Act are repeated herein as follows:

1.1.1. "**data subject**" – means the person to whom personal information relates;

1.1.2. "**personal information**" – means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to:

1.1.2.1. 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 the person;

1.1.2.2. information relating to the education or the medical, financial, criminal or employment history of the person;

1.1.2.3. any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;

1.1.2.4. the biometric information of the person;

1.1.2.5. the personal opinions, views or preferences of the person;

1.1.2.6. correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;

1.1.2.7. the views or opinions of another individual about the person; and

1.1.2.8. the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person;

1.1.3. "**processing**" – means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including:

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

1.1.3.2. dissemination by means of transmission, distribution or making available in any other form; or

1.1.3.3. merging, linking, as well as restriction, degradation, erasure or destruction of information.

1.1.4. "**record**" **–** means any recorded information:

1.1.4.1. regardless of form or medium, including any of the following:

(a) Writing on any material;

(b) 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;

(c) label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;

(d) book, map, plan, graph or drawing;

(e) 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;

1.1.4.2. in the possession or under the control of a responsible party;

1.1.4.3. whether or not it was created by a responsible party; and

1.1.4.4. regardless of when it came into existence.

1.2. In this Policy, unless the context clearly indicates a different intention, the following expressions bear the meanings given to them below and cognate expressions will have similar meanings:

1.2.1. "**Act**" – means the Protection of Personal Information Act, Act 4 of 2013, as amended;

1.2.2. "**Company**" – means IFSA (Pty) Ltd – 2000/005153/07, a private company duly incorporated under and in terms of the laws of the Republic of South Africa;

1.2.3. "**information officer**" – means the Company's information officer and deputy information officers collectively;

1.2.4. "**Policy**" – means this Policy on Lawful Processing of Personal Information.

2. OVERVIEW

2.1. The Company is a "responsible party" and/or an "operator" as defined in the Act.

2.2. The Company is committed to complying with the 8 (eight) conditions for the lawful processing of personal information, as set out in section 4(1) of the Act.

2.3. Any processing of personal information which is inconsistent with these abovementioned conditions (unless an exemption or derogation applies) will be unlawful and will give rise to penalties and/or administrative fines as provided for in the Act.

3. PURPOSE AND SCOPE

3.1. The purpose of this Policy is to provide guidance in connection with the lawful processing of personal information in and by the Company. This Policy provides the framework for the lawful processing of personal information within and by the Company.

3.2. This policy applies to the Company's directors, shareholders, employees, staff, contractors, vendors and other persons who are responsible for owning, managing, controlling and/or processing personal information within the Company.

3.3. This Policy applies to all personal information within the Company's environment and/or held by the Company.

3.4. The termination of a relationship between the Company and any person shall not affect such person's obligation to adhere to the provisions of this Policy and this Policy shall continue to have effect after such termination.

3.5. Compliance with this Policy is mandatory.

4. IMPORT OF THE 8 CONDITIONS FOR THE LAWFUL PROCESSING OF PERSONAL INFORMATION

4.1. The import of the 8 (eight) conditions for the lawful processing of personal information by or for the Company is summarised below. In applying this Policy it is important to note and understand the import of the 8 (eight) conditions for the lawful processing of personal information.

CONDITION	SUMMARY OF IMPORT
Accountability	As referred to in section 8 of the Act. In general the Company is accountable to ensure that the conditions set out in chapter 3 of the Act, and all measures that give effect to the conditions, are complied with. The obligation to process personal information lawfully cannot be contracted out, albeit by outsourcing the processing of personal information or otherwise, and as such the Company remains ultimately liable for the lawful processing of personal information by both itself and its operators. The Company is responsible and liable for the lawful processing of personal information from the time that the personal information is collected, during the time that it is processed and up to the time of its deletion/destruction. This condition works towards protecting the legitimate interests of data subjects, by providing a sort of warranty as to the security of their personal information.
Processing Limitations	As referred to in sections 9 to 12 of the Act. In general the Company must ensure that: - It processes personal information lawfully and in a reasonable manner that does not infringe the privacy of a data subject; - It processes personal information only, given the purpose for which it is processed, if such processing is adequate, relevant and not excessive; - It processes personal information only in the circumstances set out in section 11(1) of the Act; - It appropriately deals with the withdrawal of processing consents by data subjects; - It appropriately deals with the objections to processing by data subjects; - It collects personal information directly from data subjects, unless an exemption set out in terms of section 12(2) of the Act applies. The employee recruitment process could be used to illustrate the processing limitation condition. In this scenario, the Company must only access information that is relevant to the application process. Information such as a job applicant's banking details cannot be justified.
Purpose Specification	As referred to in sections 13 and 14 of the Act. In general the Company: - must only collect personal information for a specific, explicitly defined and lawful purpose; - must take reasonable steps to ensure that a data subject is aware of the purpose for the collection of the personal information, unless the provisions of section 18(4) apply;

	- must not retain personal information any longer than is necessary for achieving the purpose for which the personal information was collected or subsequently processed, unless otherwise permitted in terms of law; - must restrict the processing of personal information in circumstance contemplated in section 14(6) of the Act. Ultimately this purpose specification condition requires processing to be necessary and proportionate. Therefore this purpose specification condition ensures that processing is carried out in the least intrusive manner considering the possible security risks.
Further processing limitation	As referred to in section 15 of the Act. In general the Company is obliged to prevent the processing of information in a manner that is incompatible with the purpose for which the information was collected. Generally, this limits any secondary use of personal information, for any other purpose than the purpose for which it was collected for initial processing. This includes preventing the disclosure or transfer of personal information to third parties.
Information Quality	As referred to in section 16 of the Act. In general the Company must take reasonably practical steps to ensure that personal information is complete, accurate, not misleading and updated where necessary. It is important to note that the information quality condition is better fulfilled by ensuring that the Company is aware of the purpose for which the information is processed.
Openness	As referred to in sections 17 and 18 of the Act. In general the Company is required to ensure that data subjects are aware of the various matters related to the collection of their personal information. This involves informing them of the reasons and "destiny" of the personal information as set out in section 18(1) of the Act. It is not necessary for the Company to comply with the requirements of section 18(1) of the Act if the exemptions set out in section 18(4) of the Act apply.
Security Safeguards	As referred to in sections 19 through 22 of the Act. In general the Company must secure the integrity and confidentiality of personal information in its possession by taking appropriate reasonable and technical measures to prevent loss, damage and unlawful access. In order to do so, it is important for the Company to: - identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control; - establish and maintain appropriate safeguards against the risks identified; - regularly verify that the safeguards are effectively implemented; and - ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

	Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, the Company is obliged to discharge its notification obligations in terms of section 22 of the Act.
Data subject participation	As referred to in sections 23 through 25 of the Act. In general a data subject is entitled to: - an explanation of the personal information held by the Company about the data subject; - request information about the recipients of the data subject's personal information; and - request deletion or correction of the data subject's personal information. This participation ensures that data subjects have some measure of influence over the processing of their personal information. The condition also works to instill confidence in the data subject regarding the Company and the security of his/her personal information.

5. RULES AND PROCEDURES

5.1. The Company shall apply the following rules and procedures to ensure that it complies with the 8 (eight) conditions for the lawful processing of personal information:

5.1.1. **Responsibility and Accountability**

5.1.1.1. The Company's information officer and deputy information officers, are appointed as required in terms of the Act and the Promotion of Access to information Act ("**PAIA**").

5.1.1.2. The Company's information officer shall oversee, manage and execute this Policy and all processes and procedures required to enable privacy and data protection across the Company.

5.1.1.3. All individuals and departments within the Company, engaged and mandated by the information officer for this purpose from time to time, shall diligently and prudently assist the information officer in discharging his/her duties contemplated in 5.1.1.2 above and assumes joint responsibility and accountability with the information officer in this regard.

5.1.2. **General Obligations**

5.1.2.1. At all times during the collection and processing of personal information, a determination should be made of:

(a) the nature, scope and extent of the personal information collected and/or processed;

(b) the purposes for which the personal information is collected and/or processed; and

(c) the sources from which the personal information is collected.

5.1.2.2. Based on the determinations made under 5.1.2.1 above, it should be ensured that the collection and processing of the personal information:

(a) is lawful;

(b) is reasonable and does not infringe the privacy of data subjects; and

(c) given its purpose, is adequate, relevant and not excessive.

5.1.2.3. In complying with 5.1.2.1 and 5.1.2.2 above, regard should be had to:

(a) the obligations imposed upon the Company in respect of collecting and processing personal information; and

(b) the rights of data subjects regarding the collection and processing of their personal information;

as set out in the remainder of this Policy and the Company's *POLICY ON DATA SUBJECT RIGHTS - [ITEM NO. 2.2 OF OUR POPIA COMPLIANCE FRAMEWORK – MANDATORY ITEMS]*.

5.1.2.4. It is the responsibility of the information officer, in liaison with and supported by other individuals and departments mandated by the information officer for this purpose, to ensure that appropriate processes and procedures are developed, communicated and implemented within the Company to comply with 5.1.2.1 and 5.1.2.2 above.

5.1.3. **Specific Obligations**

5.1.3.1. *Source of Collection*

(a) Before collecting personal information, it should at the outset be determined whether same may indeed be collected from the applicable/relevant source or record intended. If the collection of personal information from a source or record other than the applicable data subject is not authorized per 5.1.3.1(b) below, the personal information shall not be collected otherwise than from the data subject direct.

(b) The Company is not permitted to collect personal information other than directly from the applicable data subject, except if:

i) the information is contained in or derived from a public record or has deliberately been made public by the data subject;

ii) the data subject or a competent person, where the data subject is a child, has consented to the collection of the information from another source;

iii) collection of the information from another source would not prejudice a legitimate interest of the data subject;

iv) collection of the information from another source is necessary:

- to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences;
- to comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Service Act, 1997 (Act No. 34 of 1997);
- for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated;
- in the interests of national security; or
- to maintain the legitimate interests of the responsible party or of a third party to whom the information is supplied;

v) collection from the data subject would prejudice a lawful purpose of the collection; or

vi) collection from the data subject is not reasonably practicable in the circumstances of the particular case.

(c) It is the responsibility of the information officer, in liaison with and supported by other individuals and departments mandated by the information officer for this purpose, to ensure that appropriate processes and procedures are developed, communicated and implemented within the Company to identify the sources from which personal information is collected and to ensure whether those sources are legitimate when measured against 5.1.3.1(a) and (b) above.

5.1.3.2. *Purpose of Collection*

(a) Before collecting personal information, it shall be ensured that same is collected for the legitimate operation and conduct of the Company's business, or for some other specific, explicitly defined and lawful purpose related to a function or activity of the Company.

(b) It is the responsibility of the information officer, in liaison with and supported by other individuals and departments mandated by the information officer for this purpose, to ensure that appropriate processes and procedures are developed, communicated and implemented within the Company to determine and ensure that personal information is collected for a specific, explicitly defined and lawful purpose related to a function or activity of the Company.

5.1.3.3. *Notification of Collection*

(a) When collecting personal information, a determination should be made on:

i) whether or not the data subject should be informed of such collection. The Company must always, unless the exceptions recorded in 5.1.3.3(f) or (g) below apply, inform the data subject of collection of his/her personal information; and

ii) if the data subject should be informed, when he/she should be informed. The timing as to when data subjects should be informed of the collection of their personal information is set out in 5.1.3.3(d) and (e).

(b) In informing a data subject of collection of his/her personal information, reasonably practicable steps must be taken to ensure that the data subject is aware of at least:

i) the personal information being collected and where the personal information is not collected from the data subject, the source from which it is collected;

ii) the name and address of the Company;

iii) the purpose for which the personal information is being collected;

iv) whether or not the supply of the personal information by that data subject is voluntary or mandatory;

v) the consequences of failure to provide the personal information;

vi) any particular law authorising or requiring the collection of the personal information;

vii) the fact that, where applicable, the Company intends to transfer the information to a third country or international organisation and the level of protection afforded to the information by that third country or international organisation;

viii) any further information such as the:

- recipient or category of recipients of the personal information;
- nature or category of the personal information;
- existence of the right of access to and the right to rectify the personal information collected;
- existence of the right to object to the processing of personal information as referred to in 5.1.4.2 and 5.1.6.4(c) below; and
- 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.

(c) The Company's *NOTIFICATION OF COLLECTION FROM - [ITEM NO. 3.2 OF OUR POPIA COMPLIANCE FRAMEWORK – MANDATORY ITEMS]* provides guidance in respect of the nature, scope and extent of notification to a data subject, for purposes of compliance, where necessary, with the Company's notification obligation expressed above.

(d) If the personal information is collected directly from the data subject, the Company's notification obligation, if any, must be discharged before the information is collected, unless the data subject is already aware of the information referred to in 5.1.3.3(b).

(e) If the personal information is collected from a source or record other than the data subject, the Company's notification obligation, if any, must be discharged before the information is collected or as soon as reasonably practicable after it has been collected. Please note paragraph 5.1.3.1(b) for circumstances where the Company may collect personal information from sources other than the data subject himself/herself.

(f) If the Company has previously notified a data subject of the collection of his/her personal information, the Company need not again take such steps in relation to the subsequent collection from the data subject of the same personal information, or personal information of the same kind, if the purpose of collection of the personal information remains the same.

(g) It is not necessary for the Company to inform a data subject of collection of his/her personal information if:

i) the data subject, or a competent person where the data subject is a child, has provided consent for the non-compliance;

ii) non-compliance would not prejudice the legitimate interests of the data subject as set out in terms of the Act;

iii) non-compliance is necessary:

- to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences;
- to comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Service Act, 1997 (Act No. 34 of 1997);

- for the conduct of proceedings in any court or tribunal that have been commenced or are reasonably contemplated; or
- in the interests of national security;

iv) compliance would prejudice a lawful purpose of the collection;

v) compliance is not reasonably practicable in the circumstances of the particular case; or

vi) the information will not be used in a form in which the data subject may be identified or will be used for historical, statistical or research purposes.

(h) It is the responsibility of the information officer, in liaison with and supported by other individuals and departments mandated by the information officer for this purpose, to ensure that appropriate processes and procedures are developed, communicated and implemented within the Company to ensure that a determination is made on whether a data subject should be notified of the collection of his personal information, and if notification is necessary that same occurs at the appropriate time.

5.1.3.4. *Processing Consent*

(a) Before processing personal information:

i) the basis upon which same is to be processed should be determined (i.e. is it based upon the consent of the data subject or otherwise). If the processing of personal information without the consent of the applicable data subject is not authorized per 5.1.3.4(b) below, the personal information shall not be processed until the data subject's consent has been obtained; and

ii) it should be determined whether there is any prohibition on the processing of the personal information as set out in 5.1.5 and/or 5.1.6 below. If there is a prohibition on the processing of the personal information as set out in 5.1.5 and/or 5.1.6 below, it should be ensured that the relevant provisions of 5.1.5 and/or 5.1.6 below are complied with to the extent necessary;

iii) it should be determined, via assessment per 5.1.3.4(f) and (g) below, whether the processing would be in accordance or compatible with the purpose for which the personal information was collected. If the processing would not be so compatible with the purpose for which the information was collected, then such processing should not be undertaken.

(b) Personal information may not be processed without the consent of a data subject, or a competent person where the data subject is a child, unless the processing of the data subject's personal information, without his/her consent, is required and/or permitted under the Act. The Act permits the processing of personal information without the consent of the data subject if:

i) processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is party;

ii) processing complies with an obligation imposed by law on the Company;

iii) processing protects a legitimate interest of the data subject; or

iv) processing is necessary for pursuing the legitimate interests of the Company or of a third party to whom the information is supplied.

(c) Where uncertainty exists about whether or not consent is necessary to process personal information, it is best practice for the Company to obtain consent. It is best practice to determine, at the time of collection of personal information, whether consent to processing is required by the Company or not.

(d) The Company bears the burden of proof for consent, and it is hence imperative that due process and care is implemented in:

i) determining whether consent to processing is required; and

ii) obtaining and recording such consent where necessary.

(e) The Company's *CONSENT TO PROCESS PERSONAL INFORMATION FROM - [ITEM NO. 3.1 OF OUR POPIA COMPLIANCE FRAMEWORK – MANDATORY ITEMS]* provides guidance in respect of the nature, scope and extent of obtaining consent from a data subject, for purposes of compliance, where necessary, with the Company's obligation to obtain such consent as expressed above.

(f) To assess whether further processing is compatible with the purpose of collection, it shall firstly be determined whether any of the circumstance listed in 5.1.3.4(g) below apply. If any of them do, then the further processing of personal information is not incompatible with the purpose of collection. If none of those circumstance apply, then, in the process of assessment, account shall be taken of:

i) the relationship between the purpose of the intended further processing and the purpose for which the information has been collected;

ii) the nature of the information concerned;

iii) the consequences of the intended further processing for the data subject;

iv) the manner in which the information has been collected; and

v) any contractual rights and obligations between the Company and data subject.

(g) The further processing of personal information is not incompatible with the purpose of collection if:

i) the data subject, or a competent person where the data subject is a child, has consented to the further processing of the information;

ii) the information is available in or derived from a public record or has deliberately been made public by the data subject;

iii) further processing is necessary:

- to avoid prejudice to the maintenance of the law by any public body including the prevention, detection, investigation, prosecution and punishment of offences;
- to comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Service Act, 1997 (Act No. 34 of 1997);
- for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated; or
- in the interests of national security;

iv) the further processing of the information is necessary to prevent or mitigate a serious and imminent threat to public health or public safety or the life or health of the data subject or another individual;

v) the information is used for historical, statistical or research purposes and the Company ensures that the further processing is carried out solely for such purposes and will not be published in an identifiable form; or

vi) the further processing of the information is in accordance with an exemption granted by the Regulator to the Company to process personal information, even if that processing is in breach of a condition for the processing of such personal information, or any measure that gives effect to such condition.

(h) It is the responsibility of the information officer, in liaison with and supported by other individuals and departments mandated by the information officer for this purpose, to ensure that appropriate processes and procedures are developed, communicated and implemented within the Company to determine and ensure that:

i) where necessary, a data subject's consent is obtained to process his personal information; and

ii) where necessary, the provisions of 5.1.5 and/or 5.1.6 below are complied with in respect of personal information where a prohibition on processing thereof exists; and

iii) processing of personal information is in accordance or compatible with the purpose for which the personal information was collected.

5.1.3.5. <u>*Quality of Information*</u>

(a) It should at all times be ensured that the personal processed by the Company from time to time is complete, accurate, not misleading and updated where necessary.

(b) It is the responsibility of the information officer, in liaison with and supported by other individuals and departments mandated by the information officer for this purpose, to ensure that appropriate processes and procedures are developed, communicated and implemented within the Company, which are aimed at:

i) informing data subjects of their obligation to provide the Company with information that is complete, accurate and not misleading;

ii) informing data subjects of their obligation to inform the Company if any of their personal information has changed; and

iii) regularly engaging data subjects with requests to ensure that their personal information held by the Company is still complete, accurate and not misleading.

5.1.3.6. <u>*Retention and Destruction*</u>

(a) Please refer the Company's *POLICY ON RETENTION AND DESTRUCTION OF RECORDS - [ITEM NO. 2.3 OF OUR POPIA COMPLIANCE FRAMEWORK – MANDATORY ITEMS]* for rules and procedures regarding the retention, restriction and destruction of records.

5.1.3.7. <u>*Security*</u>

(a) The Company must, whilst having due regard to generally accepted information security practices and procedures which may apply to it generally or which may be

required of it in terms of specific industry or professional rules and regulations, take appropriate, reasonable technical and organisational measures to prevent:

i) loss of, damage to or unauthorised destruction of personal information; and

ii) unlawful access to or processing of personal information.

(b) In order to give effect to paragraph 5.1.3.7(a), the information officer, in liaison with and supported by other individuals and departments mandated by the information officer for this purpose, must take reasonable measures to:

i) identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;

ii) establish and maintain appropriate safeguards against the risks identified;

iii) regularly verify that the safeguards are effectively implemented; and

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

(c) The information officer, in liaison with and supported by other individuals and departments mandated by the information officer for this purpose, will, in terms of a written contract between the Company and its operators, ensure that the operators, in processing personal information for the Company, establish and maintain the security measures referred to in 5.1.3.7(a) and (b) above.

(d) The Company's:

i) *EMPLOYEE ACCESS AND CONFIDENTIALITY AGREEMENT - [ITEM NO. 5.1 OF OUR POPIA COMPLIANCE FRAMEWORK – MANDATORY ITEMS]* provides guidance in respect of an agreement to be concluded with the relevant employees in the Company, in order to obtain their undertaking and commitment to the protection of personal information within and by the Company;

ii) *OPERATOR AGREEMENT - [ITEM NO. 5.2 OF OUR POPIA COMPLIANCE FRAMEWORK – MANDATORY ITEMS]* provides guidance in respect of an agreement to be concluded with the relevant operators of the Company, in order to obtain their undertaking and commitment to the protection of personal information within and by the Company.

(e) In the event of a data breach or security compromise, the Company must follow and abide by the rules and procedures set out in its *POLICY ON DATA BREACHES AND SECURITY COMPROMISES - [ITEM NO. 2.4 OF OUR POPIA COMPLIANCE FRAMEWORK – MANDATORY ITEMS]*.

5.1.4. **Specific Rights**

5.1.4.1. <u>*Consent Withdrawal*</u>

(a) On providing reasonable notice to the Company, a data subject, or a competent person where the data subject is a child, may at any time withdraw any consent given in respect of the Company's processing of the data subject's personal information.

(b) If consent to process personal information has been withdrawn, the Company may no longer process the data subject's personal information unless the processing, without consent, is required and/or permitted under the Act (refer 5.1.3.4(b)).

(c) Please refer paragraph 8 of the Company's *POLICY ON DATA SUBJECT RIGHTS - [ITEM NO. 2.2 OF OUR POPIA COMPLIANCE FRAMEWORK – MANDATORY ITEMS]* for rules and procedures regarding a data subject's withdrawal of consent to processing of personal information.

5.1.4.2. *Objection*

(a) On providing reasonable notice to the Company, a data subject, or a competent person where the data subject is a child, may at any time object to the Company's processing of the data subject's personal information.

(b) If an objection to the processing of personal information has been received, the Company may no longer process the personal information ***unless*** the processing, despite the objection, is required and/or permitted under the Act (refer 5.1.3.4(b))**.**

(c) Please refer paragraph 7 of the Company's *POLICY ON DATA SUBJECT RIGHTS - [ITEM NO. 2.2 OF OUR POPIA COMPLIANCE FRAMEWORK – MANDATORY ITEMS]* for rules and procedures regarding a data subject's objection to processing of personal information.

5.1.4.3. *Access*

(a) A data subject has the right to, either free or charge or subject to the payment of a prescribed fee, establish whether the Company holds personal information of him/her and to request access to his/her personal information.

(b) Please refer paragraph 5 of the Company's *POLICY ON DATA SUBJECT RIGHTS - [ITEM NO. 2.2 OF OUR POPIA COMPLIANCE FRAMEWORK – MANDATORY ITEMS]* for further rules and procedures regarding a data subject's request for access to personal information.

5.1.4.4. *Correction*

(a) A data subject has the right to request, where necessary, the correction, destruction or deletion of his/her personal information.

(b) Please refer paragraph 6 of the Company's *POLICY ON DATA SUBJECT RIGHTS - [ITEM NO. 2.2 OF OUR POPIA COMPLIANCE FRAMEWORK – MANDATORY ITEMS]* for further rules and procedures regarding a data subject's request for correction, deletion or destruction of personal information.

5.1.5. **Prohibition on processing of personal information**

5.1.5.1. Before processing any personal information, a determination should be made on whether such information concerns:

(a) 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

(b) 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 the disposal of such proceedings; or

(c) a child.

5.1.5.2. If personal information concerns the items or data subjects referred to in 5.1.5.1, the Company shall not process such personal information unless permitted to do so in terms of this 5.1.5.

5.1.5.3. The prohibition on processing personal information, as referred to in 5.1.5.1(a) and (b), does not apply if the:

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

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

(c) processing is necessary to comply with an obligation of international public law;

(d) processing is 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 data subject to a disproportionate extent;

(e) information has deliberately been made public by the data subject; or

(f) the Regulator has appropriately authorised the Company to process special personal information.

5.1.5.4. In addition to 5.1.5.3, the Company may process personal information concerning a data subject's religious or philosophical beliefs, as referred to in 5.1.5.1(a), if the processing is necessary to protect the spiritual welfare of the data subject, provided the data subject has not objected to the processing. Notwithstanding the fact that the Company may have the right to process personal information concerning a data subject's religious or philosophical beliefs, the Company shall not, without the data subject's prior consent, supply such information to third parties.

5.1.5.5. In addition to 5.1.5.3, the Company may process personal information concerning a data subject's race or ethnic origin, as referred to in paragraphs 5.1.5.1(a), if the processing:

(a) is carried out to identify data subjects and only when this is essential for that purpose; and

(b) complies with laws and other measures designed to protect or advance persons, or categories of persons, disadvantaged by unfair discrimination.

5.1.5.6. In addition to 5.1.5.3, the Company may process personal information concerning a data subject's political persuasion, as referred to in paragraphs 5.1.5.1(a), if the Company acts as an operator for an institution, founded on political principles, of the personal information of:

(a) its members or employees or other persons belonging to the institution, if such processing is necessary to achieve the aims or principles of the institution; or

(b) a data subject if such processing is necessary for the purposes of:

i) forming a political party;

ii) participating in the activities of, or engaging in the recruitment of members for or canvassing supporters or voters for, a political party with the view to:

- an election of the National Assembly or the provincial legislature as regulated in terms of the Electoral Act, 1998 (Act No. 73 of 1998);

- municipal elections as regulated in terms of the Local Government: Municipal Electoral Act, 2000 (Act No. 27 of 2000); or
- referendum as regulated in terms of the Referendums Act, 1983 (Act No. 108 of 1983); or

iii) campaigning for a political party or cause.

Notwithstanding the fact that the Company may have the right to process personal information concerning a data subject's political persuasion, the Company shall not, without the data subject's prior consent, supply such information to third parties.

5.1.5.7. In addition to 5.1.5.3, the Company may process personal information concerning a data subject's health or sex life, as referred to in paragraphs 5.1.5.1(a), if the processing is by:

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

(b) a private a body managing the care of a child and such processing is necessary for the performance of its lawful duties;

(c) an employer and such processing is necessary for:

i) the implementation of the provisions of laws, 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.

If the Company is entitled to process personal information in the cases referred to in this 5.1.5.7 above, the information may only be processed by the Company subject to an obligation of confidentiality established by a written agreement between the Company and the data subject. The Company must treat the information as confidential, unless the Company is required by law or in connection with its duties to communicate the information to other parties who are authorised to process such information in accordance with section 32(1) of the Act.

5.1.5.8. In addition to 5.1.5.3, the Company may process personal information concerning a data subject's criminal behaviour or biometric information, as referred to in paragraphs 5.1.5.1(b), if the Company has obtained that information in accordance with law.

5.1.5.9. The processing of information concerning personnel in the service of the Company must take place in accordance with the rules established in compliance with labour legislation.

5.1.5.10. The prohibition on processing any of the categories of personal information referred to in paragraphs 5.1.5.1(a) and (b) does not apply if such processing is necessary to supplement the processing of information on criminal behaviour or biometric information which is permitted.

5.1.5.11. The Company may process the personal information of children, as referred to in paragraph 5.1.5.1(c), if the processing is:

(a) carried out with the prior consent of a competent person;

(b) necessary for the establishment, exercise or defence of a right or obligation in law;

(c) necessary to comply with an obligation of international public law;

(d) 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; or

(e) of personal information which has deliberately been made public by the child with the consent of a competent person;

(f) the Regulator has appropriately authorised the Company to process the personal information of children.

5.1.5.12. The Company shall not, unless it has first obtained the Regulator's prior authorization:

(a) process any unique identifiers of data subjects for a purpose other than the one for which the identifier was specifically intended at collection, and with the aim of linking the information together with information processed by other responsible parties;

(b) process information on criminal behaviour or on unlawful or objectionable conduct on behalf of third parties;

(c) process information for the purposes of credit reporting; or

(d) transfer special personal information, or the personal information of children, to a third party in a foreign country that does not provide an adequate level of protection for the processing of personal information as referred to in section 72 of the Act.

The Company must obtain prior authorisation as referred to in this paragraph 5.1.5.12 only once and not each time that personal information is received or processed, except where the processing departs from that which has been authorised.

5.1.6. **Direct marketing by means of unsolicited electronic communications**

5.1.6.1. Before processing the personal information of a data subject for the purpose of direct marketing by means of any form of electronic communication, it must be determined whether the data subject:

(a) has given his/her consent to the processing; and/or

(b) is a customer of the Company.

5.1.6.2. If the data subject has not given his/her consent and he is also not a Customer of the Company, the Company shall not direct market to him/her by means of any form of electronic communication. Processing of a customer's personal information for the purpose of direct marketing by means of any form of electronic communication, shall be subject to 5.1.6.4 below.

5.1.6.3. The Company's *REQUEST FOR CONSENT TO DIRECT MARKETING FORM – [ITEM NO. 4.5 OF OUR POPIA COMPLIANCE FRAMEWORK – MANDATORY ITEMS]* provides guidance in respect of the nature, scope and extent of a request from a data subject for permission to process his personal information for the purpose of direct marketing by means of any form of electronic communication. The Company may not approach a data subject more than once in order to request his/her consent for purposes of paragraph 5.1.6.1(a) above, and may not again approach a data subject for such consent if he/she has previously withheld such consent.

5.1.6.4. If a data subject is a customer of the Company, the Company will only process his/her personal information or the purpose of direct marketing by means of any form of electronic communication:

(a) if the Company has obtained the contact details of the data subject in the context of the sale of a product or service;

(b) for the purpose of direct marketing of the Company's own or similar products or services; and

(c) if the data subject has been given a reasonable opportunity to object, free of charge and in a manner free of unnecessary formality, to such use of his, her or its electronic details:

i) at the time when the information was collected; and

ii) on the occasion of each communication with the data subject for the purpose of marketing if the data subject has not initially refused such use.

5.1.6.5. Any communication by the Company for the purpose of direct marketing must contain details of the Company's identity, and an address or other contact details to which the recipient may send a request that such communications cease.

5.1.6.6. It is the responsibility of the information officer, in liaison with and supported by other individuals and departments mandated by the information officer for this purpose, to ensure that appropriate processes and procedures are developed, communicated and implemented within the Company to ensure that:

(a) the Company's right to process personal information, for the purpose of direct marketing by means of any form of electronic communication, is properly established in all instances; and

(b) the Company properly addresses and actions any and all objections, and/or withdrawals of consent, to the Company's processing of personal information for the purpose of direct marketing by means of any form of electronic communication; and

(c) data subjects have the opportunity to opt-out of the processing of their personal information, for the purpose of direct marketing by means of any form of electronic communication, both at the time of collection of their personal information and/or at any time thereafter.

5.1.7. **Company acting as operator**

5.1.7.1. Where he Company acts as an operator for and on behalf of another responsible party, it shall aim to maintain at least the standards set out in this Policy and in the Company's *POLICY ON DATA SUBJECT RIGHTS - [ITEM NO. 2.2 OF OUR POPIA COMPLIANCE FRAMEWORK – MANDATORY ITEMS]* in processing personal information for that responsible party.

5.1.7.2. Where the Company in any way engages directly with data subjects, in the course of its mandate as an operator of another responsible party, for as far as the collection and processing of personal information is concerned, it may occur that the Company exceeds its role as a operator and itself becomes a responsible party. It should at all times be ensured that the Company is clear on whether it is a responsible party, operator and/or both when collecting and processing personal information.

5.1.7.3. Where the Company serves as an operator for another responsible party, the Company:

(a) may only process personal information received from the responsible party with the knowledge or authorisation of the responsible party, and

(b) must treat personal information which comes to their knowledge as confidential and must not disclose it unless required by law or in the course of the proper performance of its duties;

(c) notify the responsible party 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.

5.1.8. **Transfers of personal information outside South Africa**

5.1.8.1. The Company shall not transfer personal information about a data subject to a third party who is in a foreign country unless:

(a) the third party who is the recipient of the information is subject to a law, binding corporate rules or binding agreement which provide an adequate level of protection that:

i) effectively upholds principles for reasonable processing of the information that are substantially similar to the conditions for the lawful processing of personal information relating to a data subject who is a natural person and, where applicable, a juristic person; and

ii) includes provisions, that are substantially similar to this section, relating to the further transfer of personal information from the recipient to third parties who are in a foreign country;

(b) the data subject consents to the transfer;

(c) the transfer is necessary for the performance of a contract between the data subject and the Company, or for the implementation of pre-contractual measures taken in response to the data subject's request;

(d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the Company and a third party; or

(e) the transfer is for the benefit of the data subject, and:

i) it is not reasonably practicable to obtain the consent of the data subject to that transfer; and

ii) if it were reasonably practicable to obtain such consent, the data subject would be likely to give it.

5.1.8.2. The Company's *OPERATOR AGREEMENT - [ITEM NO. 5.2 OF OUR POPIA COMPLIANCE FRAMEWORK – MANDATORY ITEMS]* provides guidance in respect of an agreement to be concluded with the relevant operators of the Company, in order to obtain their undertaking and commitment to the protection of personal information within and by the Company.

5.1.8.3. It is the responsibility of the information officer, in liaison with and supported by other individuals and departments mandated by the information officer for this purpose, to ensure that appropriate processes and procedures are developed, communicated and implemented within the Company to ensure that the Company does not transfer personal information about a data subject, to a third party who is in a foreign country, in breach of 5.1.8.1 above.

6. GENERAL

6.1. All of the Company's directors, shareholders, employees, staff, contractors, vendors and other persons who are responsible for receiving and processing personal information within the Company, and all departments within the Company, will work with and assist the Company's information officer, as requested and directed by the information officer, to appropriately deal with the lawful processing of personal information.

6.2. The Company's information officer shall ensure that the Company's processing of personal information is compliant with the Act and the provisions of the policies of the Company related to the Act (including this Policy).

7. COMPLAINTS HANDLING PROCEDURE

7.1. Should a data subject be unhappy with the Company's treatment of his/her personal information or he/she believes there has been a breach of this Policy, he/she must please contact the Company's information officer and clearly set out the nature of his/her concern.

7.2. Complaints may be made orally, or in writing. Where a complaint is made orally, the data subject must confirm the complaint in writing as soon as possible. If the data subject requires assistance in lodging a complaint, he/she must please contact the Company's information officer.

7.3. A data subject's complaints will be reviewed, and the data subject will be provided with a written response within 30 (thirty) days from the date that his/her complaint has come to the attention of the Company's information officer.

7.4. Notwithstanding the above, a data subject may also choose, and he/she has the right, to lodge a complaint to the Information Regulator.

Information Officer:

Name of Information Officer:	Frederick Nicolaas van Loggerenberg
Address:	Zerwick Pavilion, Block 5, Glen Eagle Office Park, Koorsboom Anenue, Glen Marais, Kempton Park, 1619
E-Mail Address:	frikkie@ifsaplan.co.za

Deputy Information Officer:

Name of Information Officer:	Ronalda van Loggerenberg
Address:	Zerwick Pavilion, Block 5, Glen Eagle Office Park, Koorsboom Anenue, Glen Marais, Kempton Park, 1619
E-Mail Address:	ronalda@ifsaplan.co.za

Information Regulator:

Address:	JD House, 27 Stiemens Street, Braamfontein, Johannesburg, 2001
Tel No.:	+27 (0) 10 023 5200

E-Mail Address:	complaints.IR@justice.gov.za
Web Address	https://www.justice.gov.za/inforeg/contact.html

8. AMENDMENT

8.1. The Company reserves the right to amend this Policy at any time. Unless otherwise stated, the current version of this Policy from time to time shall supersede and replace all previous versions of this Policy.

9. POLICY COMPLIANCE

9.1. Compliance Measurement

9.1.2. The compliance of the Company's directors, shareholders, employees, staff, contractors, vendors and other persons who are responsible for owning, managing, controlling and/or processing personal information within the Company, shall be monitored and verified by the Company's information officer through various methods, including but not limited to, business tool reports, internal and external audits.

9.1.3. The Company implements this Policy through the use of proper procedures, including staff training, to ensure compliance with this Policy.

9.2. Exceptions

9.2.2. Any person who requires to be exempt from the provisions of this Policy, or who requires any personal information to be exempt from this Policy, shall be required to obtain prior written approval from the Company's information officer in this regard.

9.3. Non-Compliance

9.3.2. Should any of the Company's directors, shareholders, employees, staff, contractors, vendors and other persons who are responsible for owning, managing, controlling and/or processing personal information within the Company, be found to have, or be under suspicion of, violating the provisions of this Policy, the Company shall implement appropriate measures against such person, which measures may include disciplinary action, termination of employment, termination of contract, etc.

10. INFORMATION OFFICER

For further information about this Policy or to access our complaint handling procedure, please address your correspondence to the Company's information officer. Details provided above.

11. POLICY VERSION HISTORY

Version	Date	Description	Approved By
1.0	30.06.2021	First Draft	