

HUMAN NATURE CONSULTING PTY LTD

PROTECTION OF PERSONAL INFORMATION

POLICY MANUAL

and

COMPLIANCE FRAMEWORK

1. INTRODUCTION

- 1.1. This is the Policy Manual and Compliance Framework (“the/this Policy Manual”) for Human Nature Consulting Pty Ltd (“HNC”).
- 1.2. The Policy Manual has been prepared having regard to the provisions of the Protection of Personal Information Act 4 of 2013 (“POPI” or “the Act”), which regulates the collection, storage and dissemination of ‘personal information’ as defined in section 1 of POPI and set out in 2.2.6 below.
- 1.3. The conduct of the operations of HNC (described in 7 below), which are conducted in South Africa, are such that HNC is required to collect, use, store, process and share personal information of persons, including customers, suppliers, service providers and employees (the person to whom the personal information relates is referred to in POPI and in this Policy Manual as the “data subject”).
- 1.4. This Policy Manual sets out how HNC collects, uses, stores, processes and shares personal information of data subjects in compliance with the POPI.
- 1.5. This Policy Manual also sets out on **Annexure A** the HNC framework for compliance with its obligations in terms of POPI in regard to the lawful processing of personal information by HNC, and in regard to the right of data subjects to privacy and to the safeguarding of their personal information.
- 1.6. This Policy Manual is subject to review and amendment by HNC from time to time.

2. THE POPI ACT AND GUIDANCE NOTE

Purpose

- 2.1. The purpose of POPI is to:

- 2.1.1. give effect to the constitutional right to privacy, by safeguarding personal information when processed by a responsible party, such as HNC, subject to justifiable limitations that are aimed at:
 - 2.1.1.1. balancing the right to privacy against other rights, particularly the right of access to information; and
 - 2.1.1.2. protecting important interests, including the free flow of information with in the Republic of South Africa and across international borders;
- 2.1.2. regulating the manner in which personal information may be processed, by establishing conditions, in harmony with international standards, that prescribe the minimum threshold requirements for the lawful processing of personal information;
- 2.1.3. providing persons with rights and remedies to protect their personal information from processing that is not in accordance with this Act; and
- 2.1.4. establishing voluntary and compulsory measures, including the establishment of the Information Regulator, to ensure respect for and to promote, enforce and fulfil the rights protected by this Act.

Definitions

- 2.2. Definitions of words and terms used in the Act are contained in section 1 of POPI. These definitions include the following:
 - 2.2.1. “**consent**” means any voluntary, specific and informed expression of will, in terms of which permission is given for the processing of personal information;
 - 2.2.2. “**data subject**” means the person to whom personal information relates;
 - 2.2.3. “**direct marketing**” means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of:
 - 2.2.3.1. promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or
 - 2.2.3.2. requesting the data subject to make a donation of any kind for any reason;
 - 2.2.4. “**electronic communication**” means any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient’s terminal equipment until it is collected by the recipient;

- 2.2.5. “**operator**” means a person who processes personal information for HNC in terms of a contract or mandate, without coming under the direct authority of that party;
- 2.2.6. “**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:
- 2.2.6.1. 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;
 - 2.2.6.2. information relating to the education or the medical, financial, criminal or employment history of the person;
 - 2.2.6.3. any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
 - 2.2.6.4. the biometric information of the person;
 - 2.2.6.5. the personal opinions, views or preferences of the person;
 - 2.2.6.6. correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
 - 2.2.6.7. the views or opinions of another individual about the person; and
 - 2.2.6.8. the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person;
- 2.2.7. “**processing**” means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including:
- 2.2.7.1. the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation, or use;
 - 2.2.7.2. dissemination by means of transmission, distribution, or making available in any other form; or
 - 2.2.7.3. merging, linking, as well as restriction, degradation, erasure or destruction of information;
- 2.2.8. “**record**” means any recorded information:

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

2.2.8.1.1. writing on any material;

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

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

2.2.8.1.4. book, map, plan, graph or drawing;

2.2.8.1.5. photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced;

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

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

2.2.8.4. regardless of when it came into existence;

2.2.9. **“Regulator”** means the Information Regulator established in terms of section 39 of POPI;

2.2.10. **“restriction”** means to withhold from circulation, use or publication any personal information that forms part of a filing system, but not to delete or destroy such information.

Guidance Note

2.3. The Regulator issued on 1 April 2021, a Guidance note on Information Officers and Deputy Information Officers, which will be referred to in this Policy Manual as the “Guidance Note”.

3. THE INFORMATION OFFICER AND DEPUTY INFORMATION OFFICER

3.1. in terms of the POPI and in terms of the Promotion of Access to Information Act (“PAIA”) HNC being a private body in terms of POPI is required to appoint an Information Officer and to register such Information Officer with the Regulator.

3.2. HNC has appointed will an Information Officer and will have the Information Officer registered with the Regulator.

- 3.3. Where the Information Officer so appointed is not the Chief Executive Officer or the Managing Director of the company in question, such Information Officer will be appointed in writing by the relevant Chief Executive Officer or Managing Director as required in terms of POPI and the Guidance Note.
- 3.4. The Regulator will make the contact details of the Information Officer available on the Regulator's website.
- 3.5. In terms of POPI the Information Officer's responsibilities include:
 - 3.5.1. the encouragement of compliance, by HNC, with the conditions for the lawful processing of personal information;
 - 3.5.2. dealing with requests made to HNC pursuant to this Act;
 - 3.5.3. working with the Regulator in relation to investigations conducted pursuant to Chapter 6 in relation to HNC; and
 - 3.5.4. otherwise, as prescribed in POPI as amended.
- 3.6. In terms of the Regulations issued in terms of POPI the Information Officers have the following additional duties and responsibilities, namely to ensure that:
 - 3.6.1. a compliance framework is developed, implemented, monitored and maintained;
 - 3.6.2. a personal information impact assessment is done to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information;
 - 3.6.3. a manual is developed, monitored, maintained and made available as prescribed in sections 14 and 51 of PAIA, as amended;
 - 3.6.4. internal measures are developed together with adequate systems to process requests for information or access thereto;
 - 3.6.5. internal awareness sessions are conducted regarding the provisions of POPI, regulations made in terms of POPI, codes of conduct, or information obtained from the Regulator; and
 - 3.6.6. upon request by any person, copies of the manual are provided to that person upon the payment of a fee (for hardcopies) to be determined by the Regulator from time to time.
- 3.7. Where a data subject, becomes aware or suspicious of any security breach such as the unauthorised access, interference, modification, destruction or the unsanctioned disclosure of personal information, he or she must immediately report this event or suspicion to the Information Officer.

4. THE CONDITIONS FOR LAWFUL PROCESSING

4.1. The conditions for the lawful processing of personal information by a responsible party (here HNC) are set out in section 4 of POPI read together with Conditions, 1-8, in Chapter 3 (sections 8-25) of POPI.

4.2. While the Conditions are summarised below reference should be made to the provisions of the relevant sections of POPI.

4.3. Condition 1-Accountability

HNC must ensure that the conditions stipulated in Chapter 3, and all the measures that give effect to such conditions, are complied with at the time of the determination of the purpose and means of the processing and during the processing itself.

4.4. Condition 2-Processing limitation

4.4.1. Personal information must be processed lawfully and in a reasonable manner that does not infringe the privacy of the data subject.

4.4.2. Personal information may only be processed, if, given the purpose for which it is processed, it is adequate, relevant and not excessive.

4.4.3. HNC may only process personal information where:

4.4.3.1. the data subject (or a competent person where the data subject is a child) consents to the processing;

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

4.4.3.3. processing complies with an obligation imposed by law on HNC;

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

4.4.3.5. processing is necessary for pursuing the legitimate interests of HNC or other third party to whom the information is supplied.

4.4.4. Subject to section 12 of POPI, and unless compliance is not reasonably practicable in the circumstances of the particular case, personal information must be collected directly from the data subject.

4.5. Condition 3-Purpose specification

4.5.1. The functions and activities of HNC in the conduct of its business operations require that HNC collect personal information of persons, including customers, suppliers, service providers and employees.

- 4.5.2. The records of personal information must not be retained any longer than is necessary by HNC for achieving the purpose for which the information was collected or subsequently processed, unless:
 - 4.5.2.1. retention of the record is required or authorised by law;
 - 4.5.2.2. HNC reasonably requires the record for lawful purposes related to its functions or activities;
 - 4.5.2.3. retention of the record is required by a contract between the parties thereto; or
 - 4.5.2.4. the data subject (or a competent person where the data subject is a child) has consented to the retention of the record.
- 4.5.3. Where HNC has established appropriate safeguards against the records being used for any other purposes, the records of personal information may be retained for periods in excess of those contemplated in 4.5.2 (section 14 of POPI).
- 4.5.4. HNC must retain the record of personal information for such period as may be required or where no retention period is prescribed for a period which would afford the data subject a reasonable opportunity, taking all considerations relating to the use of the personal information into account, to request access to the record.
- 4.5.5. HNC must destroy or delete a record of personal information or de-identify it as soon as reasonably practicable after HNC is no longer authorised to retain the record.
- 4.5.6. The destruction or deletion of a record of personal information in terms of 4.5.5 must be done in a manner that prevents its reconstruction in an intelligible form.
- 4.5.7. HNC must restrict processing of personal information if:
 - 4.5.7.1. its accuracy is contested by the data subject for a period enabling HNC to verify the accuracy of the information;
 - 4.5.7.2. HNC no longer needs the personal information for achieving the purpose for which the information was collected or subsequently processed, but it has to be maintained for purposes of proof;
 - 4.5.7.3. the processing is alleged to be unlawful and the data subject opposes its destruction or deletion and requests the restriction of its use instead; or
 - 4.5.7.4. the data subject requests to transmit the personal data into another automated processing system.

- 4.5.8. With the processing of personal information is restricted as envisaged in 4.5.7 such information may, with the exception of storage, only be used for purposes of proof and HNC must inform the data subject before lifting the restriction on processing.

4.6. Condition 4-Further processing limitation

Further processing of personal information by HNC must be in accordance or compatible with the purpose for which HNC collected the information. In assessing whether further processing is compatible with the purpose of collection HNC must take into account the provisions of section 15 (2) and (3).

4.7. Condition 5-Information quality.

- 4.7.1. Having regard to the purpose for which HNC collected or further processed the personal information, HNC must take reasonably practicable steps to ensure that the personal information is complete, accurate, not misleading and updated where necessary.
- 4.7.2. Where personal information is collected or received from third parties, HNC will take reasonable steps to confirm that the information is correct by verifying the accuracy of the information directly with the data subject or by way of independent sources.

4.8. Condition 6-Openness

- 4.8.1. Documentation of all processing operations under its responsibility must be maintained by HNC as referred to in section 14 or section 51 of PAIA.
- 4.8.2. Where HNC collects personal information, HNC must take reasonably practicable steps, before the personal information is collected if directly from the data subject, to ensure that the data subject is aware of:
- 4.8.2.1. the information being collected, and if not from the data subject, the source from which it is collected;
 - 4.8.2.2. the name and address of HNC;
 - 4.8.2.3. the purpose for which the information is being collected;
 - 4.8.2.4. whether or not the supply of the information by that data subject is voluntary or mandatory;
 - 4.8.2.5. the consequences of failure to provide the information;

- 4.8.2.6. any particular law authorising or acquiring the collection of the information;
- 4.8.2.7. HNC in the course of its operations does not transfer personal information of its data subjects outside of South Africa;
- 4.8.2.8. the fact that, where applicable, HNC does in future intend 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 will be dealt with in compliance of section 72 of POPI;
- 4.8.2.9. any further information, such as the:
 - 4.8.2.9.1. recipient or category of recipients of the information;
 - 4.8.2.9.2. nature or category of the information;
 - 4.8.2.9.3. existence of the right of access to, and the right to rectify, the information collected;
 - 4.8.2.9.4. existence of the right to object to the processing of personal information as referred to in section 11 (3) of POPI; and
 - 4.8.2.9.5. 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 information is or is not to be processed, to enable processing in respect of the data subject to be reasonable.

4.8.3. The circumstances in which it will not be necessary for HNC to comply with the requirements set out in 4.8.2 are contained in section 18 (4) of POPI.

4.9. Condition 7-Security Safeguards

- 4.9.1. HNC must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent;
 - 4.9.1.1. loss of, damage to or unauthorised destruction of personal information; and
 - 4.9.1.2. unlawful access to or processing of personal information.
- 4.9.2. In order to comply with 4.9.1 HNC, having regard to generally accepted information security practices and procedures, must take reasonable measures to:

- 4.9.2.1. identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;
 - 4.9.2.2. establish and maintain appropriate safeguards against the risks identified;
 - 4.9.2.3. regularly verify that the safeguards are effectively implemented; and
 - 4.9.2.4. ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.
- 4.9.3. Unless required by law, or in the course of the proper performance of their duties, an operator or anyone processing personal information on behalf of HNC must:
- 4.9.3.1. process such information only with the knowledge or authorisation of HNC; and
 - 4.9.3.2. treat personal information, which comes to their knowledge as confidential and must not disclose it.
- 4.9.4. HNC must, in terms of a written contract between HNC and the operator, ensure that the operator, which processes personal information for HNC establishes and maintains the security measures referred to in 4.9.1 (section 19 of POPI). The operator must notify HNC immediately where there are reasonable grounds to believe that the personal information of the data subject has been accessed or acquired by any unauthorised person.
- 4.9.5. Where there are reasonable grounds to believe that the personal information of the data subject has been accessed or acquired by any unauthorised person HNC must notify the Regulator and the data subject on the basis set out in section 22 of POPI. This notification will be done in terms of the Compliance Framework provisions set out below.
- 4.9.6. HNC's operators and third-party service providers will be required to enter into service level agreements with the organisation where both parties pledge their mutual commitment to POPIA and the lawful processing of any personal information pursuant to the agreement.

4.10. Condition 8-Data subject participation.

- 4.10.1. A data subject, having provided HNC adequate proof of identity, has the right to:

- 4.10.1.1. request HNC to confirm, free of charge, whether or not HNC holds personal information about the data subject; and
- 4.10.1.2. request from HNC the record, or a description of the personal information about the data subject held by HNC, including information about the identity of all third parties, or categories of third parties, who have, or have had, access to the information.
- 4.10.2. Where such a request is made, HNC must provide the information within a reasonable time, at a prescribed fee (if any), in a reasonable manner and format and in a form that is generally understandable.
- 4.10.3. Requests made will be processed in accordance with section 23 of POPI and the Compliance Framework provisions set out below.
- 4.10.4. The provisions of sections 18 and 53 of PAIA (form of requests) apply to requests made in terms of section 23 of POPI.
- 4.10.5. The data subject has the right to request HNC to correct or delete personal information about the data subject in its possession or under its control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully and the right to request HNC to destroy or delete a record of personal information about the data subject that HNC is no longer authorised to retain. HNC must respond to that request in terms of section 24 of POPI and the Compliance Framework provisions set out below.

5. PROCESSING OF SPECIAL PERSONAL INFORMATION

- 5.1. HNC will comply with the provisions of Part B (sections 26-33) of POPI which deal with the prohibition on processing of special personal information concerning data subjects, including children, concerning:
 - 5.1.1. 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
 - 5.1.2. the criminal behaviour of a data subject to the extent that such information relates to:
 - 5.1.2.1. the alleged commission by a data subject of any offence; or
 - 5.1.2.2. any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

6. SUPERVISION

- 6.1. The Information Regulator has been established in terms of POPI having the powers, duties and functions to:
- 6.1.1. provide education;
 - 6.1.2. monitor and enforce compliance;
 - 6.1.3. consult with interested parties;
 - 6.1.4. handle complaints;
 - 6.1.5. conduct a research and to report to Parliament;
 - 6.1.6. issue codes of conduct as envisaged in Chapter 7 of POPI;
 - 6.1.7. facilitate cross-border co-operation; and
 - 6.1.8. generally, take such steps as are required to carry out the duties and functions of the Regulator in accordance with the powers given to the Regulator.

7. OPERATIONAL CONSIDERATIONS

- 7.1. The operations of HNC involve the provision of consulting services, project management, B-BBEE consulting services, funding proposal assistance and skills development with a view to grow and support partnerships between private entities and individuals in order to establish sustainable impacts in South Africa and beyond.
- 7.2. In the course of the conduct of the operations of HNC, it is necessary for HNC to collect, use, store, process and share personal information of persons, including customers, suppliers, service providers and employees.
- 7.3. Given the nature of the operations of HNC, which include retaining personal information in order to:
- 7.3.1. Deliver services to the HNC clients;
 - 7.3.2. meet statutory obligations;
 - 7.3.3. have the personal information available for historical, statistical or research purposes;
 - 7.3.4. have the personal information available as evidence in regard to possible litigation between HNC and the data subject;
 - 7.3.5. deal with the relationship between HNC and its employees and ex-employees; and
 - 7.3.6. meet any other obligations of HNC arising from the conduct of its operations,

HNC may retain the personal information for periods in excess of those prescribed in POPI and elsewhere where HNC has established appropriate

safeguards against the records being used for any other purposes under conditions of restriction determined by HNC.

- 7.4. Documentation used by HNC, which calls for personal information to be supplied will contain a consent clause, meeting the requirements of POPI in which the data subject, providing the personal information consents to the collection, using, storing, processing and sharing of the personal information by HNC.
- 7.5. Employees who are required to have access to, and to process, personal information of data subject shall be trained in regard to the requirements of POPI and the steps to be taken in order to ensure compliance. Employees who act in breach of the provisions of POPI and this Policy Manual and Compliance Framework will face disciplinary action.

8. DIRECT MARKETTING

- 8.1. HNC will not undertake the processing of personal information of a data subject for the purpose of direct marketing by means of any form of electronic communication, including automatic calling machines, facsimile machines, SMS's or e-mail unless the data subject:
 - 8.1.1. has given his, her or its consent (in the prescribed manner and form) to the processing; or
 - 8.1.2. is a client of HNC but subject to the provisions of 8.2 below.
- 8.2. HNC may process the personal information of a data subject who is a client of HNC:
 - 8.2.1. if HNC has obtained the contact details of the data subject in the context of the sale of a product or service;
 - 8.2.2. for the purpose of direct marketing of HNC's services; and
 - 8.2.3. 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:
 - 8.2.3.1. at the time when the information was collected; and
 - 8.2.3.2. 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.
- 8.3. Any communication for the purpose of direct marketing must contain;
 - 8.3.1. details of the identity of the sender or the person on whose behalf the communication has been sent; and

- 8.3.2. an address or other contact details to which the recipient may send a request that such communications cease.

9. COMPLIANCE FRAMEWORK

Attached as **Annexure A** is a copy of the HNC Compliance Framework.

Annexure A to HNC Policy Manual

COMPLIANCE FRAMEWORK

Introduction

10. This Framework sets out in outline the steps that have been taken, and will be taken, by HNC in order to ensure compliance with its obligations in terms of POPI. This Framework is subject to review and amendment by HNC from time to time.

Information Officer

11. HNC will appoint an Information Officer as set out above in accordance with POPI and the Guidance Note.
12. The Information Officer:
 - 12.1. has developed this Policy Manual and Compliance Framework as envisaged in clauses 6.2.1 and 6.2.3 of the Guidance Note;
 - 12.2. has undertaken a personal information impact assessment to ensure that adequate measures and standards exist in order for HNC to comply with the conditions for the lawful processing of personal information, which measures and standards will be reviewed from time to time;
 - 12.3. has developed internal measures, together with adequate systems to process requests for information or access thereto;
 - 12.4. has arranged for internal awareness sessions to be conducted in HNC regarding the provisions of POPI, regulations made in terms of POPI, codes of conduct, or information obtained from the Regulator and will arrange for further internal awareness sessions from time to time as required; and

- 12.5. will arrange to provide a copy of this Policy Manual to any person requesting a copy upon the payment of a fee (if hard copies are to be supplied) to be determined by the Regulator from time to time; and
- 12.6. will comply with requests from the Regulator in terms of section 83 (4) of PAIA to furnish the Regulator with information about requests for access to records of HNC.

Security compromise

- 13. The Information Officer will prepare an Initial Response Plan setting out the procedures to be followed in the event of there being a security compromise.
- 14. Any employee of HNC who suspects that there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person must immediately notify the Information Officer (with such notification being confirmed thereafter in writing) of the possible security compromise.
- 15. Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, HNC will notify the Regulator, and subject to the provisions of section 22 (3) of POPI, the data subject, unless the identity of such data subject cannot be established. Such notification:
 - 15.1. must be made as soon as reasonably possible after the discovery of the compromise, having regard to the provisions of section 22 (2) of POPI, and may only be delayed on the grounds set out in terms of section 22 (3) of POPI;
 - 15.2. must be in writing and be communicated to the data subject in at least one of the following ways:
 - 15.2.1. mailed to the data subject's last known physical or postal address;
 - 15.2.2. sent by e-mail to the data subject's last known e-mail address;
 - 15.2.3. placed in a prominent position on the website of the responsible party;
 - 15.2.4. published in the news media; or
 - 15.2.5. as may be directed by the Regulator;
 - 15.3. must provide sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise, including:
 - 15.3.1. a description of the possible consequences of the security compromise;
 - 15.3.2. a description of the measures that HNC intends to take or has taken to address the security compromise;

15.3.3. a recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise;

15.3.4. if known to HNC, the identity of the unauthorised person who may have accessed or acquired the personal information.

Collection and processing of personal information

16. In regard to the collection and processing of personal information of data subjects. Compliance requires that;

16.1. personal information of a data subject will only be collected and processed with the consent of the data subject as required in terms of POPI;

16.2. such consent is to be obtained in writing, or by means of electronic communication, at the first point of contact with the data subject, or as soon as practicable thereafter;

16.3. in regard to customers this will take place when dealing with the customer;

16.3.1. in person;

16.3.2. by electronic communication;

16.3.3. at the time when the customer applies for an account with HNC;

16.3.4. at the time when the customer applies for and FHC Trade Card;

16.3.5. at the time when the customer applies for a quotation to be issued by HNC; or

16.3.6. at the time when the customer contacts HNC for the purposes of doing business with HNC.

16.4. In regard to suppliers of goods and services to HNC this will be at the time when HNC contracts with the supplier.

16.5. In regard to service providers to HNC this will be at the time when HNC contracts with the service provider.

16.6. In regard to applicants for employment by HNC this will be at the time when application for employment is made by the applicant.

16.7. In regard to employees of HNC this will be at the time of their appointment as employee.

16.8. Initial awareness sessions have already been undertaken in regard to POPI and in regard to this Policy Manual.

Training

17. The Information Officer will arrange for ongoing training sessions in regard to POPI and this Policy Manual particularly in regard to those employees who are involved in the collection, use, storing, processing and/or sharing personal information of data subjects in the course of the operations of HNC.

Dealing with requests from data subjects

18. The Information Officer will prepare a Request Response Plan which will set out the steps to be followed in the event of a data subject making a request for access to personal information relating to that data subject and/or for the correction of personal information as envisaged in section 23 of POPI. This Request Response Plan will include:
- 18.1. the requirement that any request for access to personal information received by any employee of the HNC be directed to the Information Officer; that the only party to respond will be the Information Officer, or someone delegated by the Information Officer to respond to that request;
 - 18.2. the request will be considered having regard to the provisions of POPI and the form and nature of the request;
 - 18.3. the Information Officer will decide in regard to the request in accordance with the requirements of POPI and will thereafter respond to the data subject accordingly;
 - 18.4. the Information Officer will respond to the data subject in regard to any request for the correction of personal information of the data subject on the basis set out in section 24 of POPI.

Method of recording personal information

19. Personal information required by HNC for the conducting of its operations will be recorded in the following formats:
- 19.1. hardcopy; and/or
 - 19.2. in digital format.
20. The Information Officer will determine where copies of personal information are to be kept, when recorded in hard copy format, and the manner of recording personal information in digital format.
21. Procedures will be determined by the Information Officer for the storage of hard copies and digital copies of the personal information where this is to be kept in order to comply with statutory requirements placed on HNC, or for such longer period as HNC requires to retain the records of personal information as envisaged in section 14 (2) of POPI.
22. Such storage must be undertaken in a way where the records of personal information of a data subject can be retrieved when required in terms of POPI or for purposes of correction, restriction, degradation, erasure or destruction of information.
23. Where hard copies of personal information are to be destroyed this will either be done by HNC, or by a third-party service provider appointed for this purpose. The

appointment of such service provider will be in terms of a written contract requiring the service provider (unless required by law in the course of the proper performance of the service provider's duties):

23.1. to process such information only with the knowledge of and authorisation of HNC in accordance with the provisions of the written contract; and

23.2. to treat personal information, which comes to the knowledge of the service provider is confidential being information not to be disclosed.

24. Where digital copies of personal information are to be destroyed this will either be done by HNC, or by a third-party service provider appointed for this purpose. The appointment of such service provider will be in terms of a written contract requiring the service provider (unless required by law in the course of the proper performance of the service provider's duties):

24.1. to process such information only with the knowledge of and authorisation of HNC in accordance with the provisions of the written contract; and

24.2. to treat personal information, which comes to the knowledge of the service provider is confidential being information not to be disclosed.

Annexure A to HNC Policy Manual

COMPLIANCE FRAMEWORK

Introduction

25. This Framework sets out in outline the steps that have been taken, and will be taken, by HNC in order to ensure compliance with its obligations in terms of POPI.

This Framework is subject to review and amendment by HNC from time to time.

Information Officer

26. HNC will appoint an Information Officer as set out above in accordance with POPI and the Guidance Note.

27. The Information Officer:

27.1. has developed this Policy Manual and Compliance Framework as envisaged in clauses 6.2.1 and 6.2.3 of the Guidance Note;

27.2. has undertaken a personal information impact assessment to ensure that adequate measures and standards exist in order for HNC to comply with the

- conditions for the lawful processing of personal information, which measures and standards will be reviewed from time to time;
- 27.3. has developed internal measures, together with adequate systems to process requests for information or access thereto;
- 27.4. has arranged for internal awareness sessions to be conducted in HNC regarding the provisions of POPI, regulations made in terms of POPI, codes of conduct, or information obtained from the Regulator and will arrange for further internal awareness sessions from time to time as required; and
- 27.5. will arrange to provide a copy of this Policy Manual to any person requesting a copy upon the payment of a fee (if hard copies are to be supplied) to be determined by the Regulator from time to time; and
- 27.6. will comply with requests from the Regulator in terms of section 83 (4) of PAIA to furnish the Regulator with information about requests for access to records of HNC.

Security compromise

28. The Information Officer will prepare an Initial Response Plan setting out the procedures to be followed in the event of there being a security compromise.
29. Any employee of HNC who suspects that there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person must immediately notify the Information Officer (with such notification being confirmed thereafter in writing) of the possible security compromise.
30. Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, HNC will notify the Regulator, and subject to the provisions of section 22 (3) of POPI, the data subject, unless the identity of such data subject cannot be established. Such notification:
- 30.1. must be made as soon as reasonably possible after the discovery of the compromise, having regard to the provisions of section 22 (2) of POPI, and may only be delayed on the grounds set out in terms of section 22 (3) of POPI;
- 30.2. must be in writing and be communicated to the data subject in at least one of the following ways:
- 30.2.1. mailed to the data subject's last known physical or postal address;
- 30.2.2. sent by e-mail to the data subject's last known e-mail address;
- 30.2.3. placed in a prominent position on the website of the responsible party;
- 30.2.4. published in the news media; or

- 30.2.5. as may be directed by the Regulator;
- 30.3. must provide sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise, including:
 - 30.3.1. a description of the possible consequences of the security compromise;
 - 30.3.2. a description of the measures that HNC intends to take or has taken to address the security compromise;
 - 30.3.3. a recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise;
 - 30.3.4. if known to HNC, the identity of the unauthorised person who may have accessed or acquired the personal information.

Collection and processing of personal information

- 31. In regard to the collection and processing of personal information of data subjects. Compliance requires that;
 - 31.1. personal information of a data subject will only be collected and processed with the consent of the data subject as required in terms of POPI;
 - 31.2. such consent is to be obtained in writing, or by means of electronic communication, at the first point of contact with the data subject, or as soon as practicable thereafter;
 - 31.3. in regard to customers this will take place when dealing with the customer;
 - 31.3.1. in person;
 - 31.3.2. by electronic communication;
 - 31.3.3. at the time when the customer applies for an account with HNC;
 - 31.3.4. at the time when the customer applies for and FHC Trade Card;
 - 31.3.5. at the time when the customer applies for a quotation to be issued by HNC; or
 - 31.3.6. at the time when the customer contacts HNC for the purposes of doing business with HNC.
 - 31.4. In regard to suppliers of goods and services to HNC this will be at the time when HNC contracts with the supplier.
 - 31.5. In regard to service providers to HNC this will be at the time when HNC contracts with the service provider.
 - 31.6. In regard to applicants for employment by HNC this will be at the time when application for employment is made by the applicant.

31.7. In regard to employees of HNC this will be at the time of their appointment as employee.

31.8. Initial awareness sessions have already been undertaken in regard to POPI and in regard to this Policy Manual.

Training

32. The Information Officer will arrange for ongoing training sessions in regard to POPI and this Policy Manual particularly in regard to those employees who are involved in the collection, use, storing, processing and/or sharing personal information of data subjects in the course of the operations of HNC.

Dealing with requests from data subjects

33. The Information Officer will prepare a Request Response Plan which will set out the steps to be followed in the event of a data subject making a request for access to personal information relating to that data subject and/or for the correction of personal information as envisaged in section 23 of POPI. This Request Response Plan will include:

33.1. the requirement that any request for access to personal information received by any employee of the HNC be directed to the Information Officer; that the only party to respond will be the Information Officer, or someone delegated by the Information Officer to respond to that request;

33.2. the request will be considered having regard to the provisions of POPI and the form and nature of the request;

33.3. the Information Officer will decide in regard to the request in accordance with the requirements of POPI and will thereafter respond to the data subject accordingly;

33.4. the Information Officer will respond to the data subject in regard to any request for the correction of personal information of the data subject on the basis set out in section 24 of POPI.

Method of recording personal information

34. Personal information required by HNC for the conducting of its operations will be recorded in the following formats:

34.1. hardcopy; and/or

34.2. in digital format.

35. The Information Officer will determine where copies of personal information are to be kept, when recorded in hard copy format, and the manner of recording personal information in digital format.

36. Procedures will be determined by the Information Officer for the storage of hard copies and digital copies of the personal information where this is to be kept in

order to comply with statutory requirements placed on HNC, or for such longer period as HNC requires to retain the records of personal information as envisaged in section 14 (2) of POPI.

37. Such storage must be undertaken in a way where the records of personal information of a data subject can be retrieved when required in terms of POPI or for purposes of correction, restriction, degradation, erasure or destruction of information.
38. Where hard copies of personal information are to be destroyed this will either be done by HNC, or by a third-party service provider appointed for this purpose. The appointment of such service provider will be in terms of a written contract requiring the service provider (unless required by law in the course of the proper performance of the service provider's duties):
 - 38.1. to process such information only with the knowledge of and authorisation of HNC in accordance with the provisions of the written contract; and
 - 38.2. to treat personal information, which comes to the knowledge of the service provider is confidential being information not to be disclosed.
39. Where digital copies of personal information are to be destroyed this will either be done by HNC, or by a third-party service provider appointed for this purpose. The appointment of such service provider will be in terms of a written contract requiring the service provider (unless required by law in the course of the proper performance of the service provider's duties):
 - 39.1. to process such information only with the knowledge of and authorisation of HNC in accordance with the provisions of the written contract; and
 - 39.2. to treat personal information, which comes to the knowledge of the service provider is confidential being information not to be disclosed.

