



NAMC

Promoting market access for South African agriculture

NAMC POPI POLICY


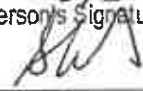
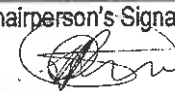
NATIONAL AGRICULTURAL MARKETING COUNCIL
Business Office

Block A | 4th floor | Meintjiesplein Building | 536 Francis Baard Street | Arcadia | Pretoria | 0002.
Private Bag X935 | Pretoria | 0001
Tel: 012 341 1115 | Fax: 012 341 1811
www.namc.co.za

NAMC POPI POLICY

Policy No	POPI/07/2021
Effective date	August 2021
Policy application	To all NAMC staff and stakeholders
Managed by	Information Officer

CONTROL MEASURES OF THE POLICY

Recommended by: Chief Executive Officer	Date 28-01-2022	Chief Executive Officer's Signature: 
Recommended by: Audit and Risk Committee	Date	Chairperson's Signature 
Approved by: Council	Date	Chairperson's Signature 
Next Review Date	Date 05 June 2022	Annually

REVISION RECORD

Date	Revision Description

TABLE OF CONTENTS

1. PREAMBLE.....	6
2. PURPOSE.....	6
3. ORGANISATIONAL SCOPE.....	7
4. RIGHTS OF DATA SUBJECTS	8
4.1.1. The rights to access personal information.....	8
4.1.2. The right to have personal information corrected or deleted	9
4.1.3. The right to object to the processing of Personal Information	9
4.1.4. The right to object to Direct Marketing	9
4.1.5. The right to complain to the Information Regulator	9
4.1.6. The right to be informed.....	10
5. GENERAL GUIDING PRINCIPLES	10
5.1.1. Accountability	10
5.1.2. Processing limitation	10
5.1.3. Purpose Specifications	11
5.1.4. Further processing limitation.....	12
5.1.5. Information Quality	12
5.1.5. Open Communication	12
5.1.6. Security Safeguards.....	13
5.1.7. Data subject participation	14
6. INFORMATION OFFICERS.....	14
7. SPECIFIC DUTIES AND RESPONSIBILITIES	15
7.1. Governing Body	15
7.2. Information Officer	15
7.3. Employees and other persons acting on behalf of NAMC	17
8. POPIA AUDIT.....	21
9. REQUEST TO ACCESS PERSONAL INFORMATION	21
10. POPIA COMPLAINTS PROCEDURE	22
11. DISCIPLINARY ACTION.....	24
12. LEGISLATIVE FRAMEWORK.....	24
13. REFERENCES.....	24
14. APPROVAL STRUCTURES	25

ABBREVIATIONS / ACRONYMS	
DALRRD	Department of Agriculture, Department of Agriculture, Land Reform and Rural Development
The Council	Council Members
A&RC	Audit and Risk Committee
CEO	Chief Executive Officer
CFO	Chief Financial Officer
AG	Auditor General of South Africa
MAP Act	Marketing of Agricultural Products Act
PFMA	Public Finance Management Act
NAMC	National Agricultural Marketing Council.
I/A	Internal Auditors
ISPPIA	International Standards of Professional Practice of Internal Auditing
Management Committee ("MANCOM")	The CEO, who is the chairperson of the committee, Chief Financial Officer, and all other Senior Managers
SAICA	South African Institute of Chartered Accountants
TR	National Treasury Regulations
King IV	King IV code of Corporate Governance Principles 2016

DEFINITION OF TERMS

- a) **Consent:** Any voluntary, specific and informed expression of will in terms of which
- b) **Data subject:** The person to whom personal information relates
- c) **Direct marketing:** To approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of – (a) promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or (b) requesting the data subject to make a donation of any kind for any reason.
- d) **Electronic communication:** the recipient collects 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.
- e) **Enforcement notice:** A notice issued in terms of section 95.
- f) **Information Officer:** Of, or in relation to, (a) public body means an information officer or deputy information officer as contemplated in terms of section 1 or 17; or (b) private body means the head of a private body as contemplated in section 1, of the Promotion of Access to Information Act.
- g) **Minister:** A Cabinet member responsible for the administration of justice.
- h) **Operator:** A person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party.
- i) **Person:** A natural person or a juristic person.
- j) **Personal information:** Information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to: (a) 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; (b) Information

relating to the education or the medical, financial, criminal or employment history of the person; (c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person; (d) The biometric information of the person; (e) The personal opinions, views or preferences of the person; (f) 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; (g) The views or opinions of another individual about the person; and (h) 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.

k) Prescribed: Prescribed by regulation or code of conduct.

l) Promotion of Access to Information Act: The Promotion of Access to Information Act, 2000 (Act No. 2 of 2000).

m) Regulator: The Information Regulator established in terms of section 39.

n) Responsible party: A public or private body or any other person, which, alone or in conjunction with others, determines the purpose of and means for processing personal information.

o) Unique identifier: Any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party.

1. PREAMBLE

- 1.1. The right to privacy is an integral human right recognised and protected in South African Constitution and in the Protection of Personal information Act 4 of 2013 (“POPIA”).
- 1.2. POPIA aims to promote the protection of privacy through providing guiding principles that are intended to be applied to the processing of personal information in a context-sensitive manner.
- 1.3. Through the provision of quality goods and services, NAMC is necessarily involved in the collection, use and disclosure of certain aspects of personal information of clients, customers, employees and other stakeholders.
- 1.4. A person’s right to privacy entails having control over his or her personal information and being able to conduct his or her affairs relatively free from unwanted intrusions.
- 1.5. Given the importance of privacy, NAMC is committed to effectively managing personal information in accordance with POPIA’s provisions.

2. PURPOSE

- 2.1. The purpose of this policy is to protect NAMC from the compliance risk associated with the protection of personal information, which includes:
 - a) Breaches of confidentiality. For instance, NAMC could suffer loss in revenue where it is found that the personal information of data subjects has been shared or disclosed inappropriately.
 - b) Failing to offer choice. For instance, all data subjects should be free to choose how and for what purpose NAMC uses information relating to them.
 - c) Reputational damage. For instance, the organisation could suffer a decline in reputational value following an adverse event such as computer hacker deleting personal information held by NAMC.

2.2. This policy demonstrates NAMC's commitment to protecting the privacy rights of data subjects in the following manner:

- a) Through stating desired behaviour and directing compliance with the provisions of POPIA and best practice.
- b) By cultivating an organisational culture that recognises privacy as a valuable human right.
- c) By developing and implementing internal controls for managing, the compliance risk associated with the protection of personal information.
- d) By creating business practices that will provide reasonable assurance that the rights of data subjects are protected and balanced with legitimate business needs of NAMC.
- e) By assigning specific duties and responsibilities to control owners, including the appointment of an Information Officer and where necessary, Deputy Information Officer in order to protect the interests of NAMC and data subjects.
- f) By raising awareness through training and providing guidance to individuals who process personal information so that they can act confidently and consistently.

3. ORGANISATIONAL SCOPE

3.1. This policy and its guiding principles apply to:

- a) NAMC's Council
- b) All Campuses, business units and divisions of NAMC.
- c) All employees and service providers and clients.
- d) All contractors, suppliers and other persons acting on behalf of NAMC.

- 3.2. This policy's guiding principles find application in all situations and must be read in all conjunction with POPIA as well as the organisation's PAIA Policies as required by the Promotion of Access to Information Act (Act No 2 of 2000).
- 3.3. The legal duty to comply with POPIA's provisions is activated in any situations where there is:
- a) A **processing** of
 - b) **Personal information**
 - c) Entered to a **record**
 - d) by or for a **responsible person**
 - e) who is **domiciled** in South Africa
- 3.4. POPIA does not apply in situations where the processing of personal information:
- a) Is concluded in the course of purely personal or household activities
 - b) Where the personal information has been de-identified.

4. RIGHTS OF DATA SUBJECTS

- 4.1. Where appropriate, NAMC will ensure that its clients and customers are made aware of the rights conferred upon them as data subjects. NAMC will ensure that it give effects to the following seven rights:

4.1.1. The rights to access personal information

- a) NAMC recognises that a data subject has the right to establish whether NAMC holds personal information related to him, her or it including the right to request access to that personal information. An example of "Personal Information Access Form "can be found under **Annexure A**.

4.1.2. The right to have personal information corrected or deleted

- a) The data subject has the right to request, where necessary that his, or her its personal information must be corrected or deleted where NAMC is no longer authorised to retain the personal information.

4.1.3. The right to object to the processing of Personal Information

- a) The data subject has the right, on reasonable grounds, to object to the processing of his or her, or its personal information.
- b) In such circumstances, NAMC will give due consideration to the request and requirements of POPIA. NAMC may cease to use or disclose the data subject's personal information and may, subject to any statutory and contractual record keeping requirements, also approve the destruction of personal information.

4.1.4. The right to object to Direct Marketing

- a) The data subject has the right to object to the processing of his or her, or its personal information for purpose of direct marketing by means of unsolicited electronic communications.

4.1.5. The right to complain to the Information Regulator

- a) The data subject has the right to submit a complaint to the Information Regulator regarding an alleged infringement of any of the rights protected under POPIA and to institute civil proceedings regarding the alleged non-compliance with the protection of his, her or its personal information.
- b) An example of "POPIA complaint form" can be found on **Annexure B**.

4.1.6. The right to be informed

- a) The data subject has the right to be notified that his, her or its personal information is been by collected NAMC. The data subject has the right to be notified in any situation where NAMC has reasonable grounds to believe that the personal information of the data subject has been accessed or acquired by an unauthorised person.

5. GENERAL GUIDING PRINCIPLES

- 5.1. All employees and persons acting on behalf of NAMC will at all times be subject to, an act in accordance with, the following guiding principles:

5.1.1. Accountability

- a) Failing to comply with POPIA could potentially damage NAMC's reputation or expose the organisation to a civil claim for damages. The protection of personal information therefore everybody's responsibility.
- b) NAMC will ensure that the provision of POPIA and the guiding principles outlined in this policy are complied with through the encouragement of desired behaviour. However, NAMC will take appropriate sanctions, which may include disciplinary action, against those individuals through their intentional or negligent actions and /or omissions fail to comply with the principles and responsibilities outlined in this policy.

5.1.2. Processing limitation

- a) NAMC will ensure that personal information under its control is processed: in a fair, or lawful and non- excessive manner and, only with the consent of data subject and, only for a specific defined purpose.
- b) NAMC will inform the data subject of the reasons for collecting his, her or its personal information and obtain written consent prior to processing personal information.
- c) Alternatively, where services or transactions are concluded over the telephone or electronic video feed, NAMC will maintain a voice recording of the stated purpose for collecting the personal information followed by the data's subject 's subsequent consent.
- d) NAMC will under no circumstances distribute or share personal information between separate legal entities, associated organisations (such as subsidiary companies) or with any individuals that are not directly involved with facilitating the purpose for which the information was originally collected.
- e) Where applicable, the data subject must be informed of the possibility that their personal information will be shared with other aspects of the organisation's business and be provided with the reasons for doing so.
- f) An example of "POPIA Notice and Consent Form "can be found under **Annexure C**.

5.1.3. Purpose Specifications

- a) All NAMC's business units and operations must be informed by the principle of transparency.
- b) NAMC will process personal information only for specific, explicitly defined and legitimate reasons.
- c) NAMC will inform data subjects of these reasons prior to collecting or recording the data subject's personal information.

5.1.4. Further processing limitation

- a) Personal information will not be processed for secondary purpose unless the processing is compatible with the original purpose. Therefore, where NAMC seeks to process personal information, it holds for a purpose other than the original purpose for which it was originally collected, and where this secondary purpose is not compatible with the original purpose, NAMC will first obtain additional consent from the data subject.

5.1.5. Information Quality

- a) NAMC will take responsible steps to ensure that all personal information collected is complete, accurate and not misleading.
- b) The more important it is that the personal information be accurate (for example, the beneficiary details of a life insurance policy are the utmost importance), the greater the effort the organisation will put to into ensuring its accuracy.
- c) Where personal information is collected or received, from third parties, NAMC will take reasonable steps to confirm that the information is correct by verifying the accuracy of information directly with the data subject or by way of independent sources.

5.1.5. Open Communication

- a) NAMC will take reasonable steps to ensure that data subjects are notified (are at all times aware) that their personal information is been collected including the purpose for which it is been collected and processed.
- b) NAMC will ensure that it establishes and maintains a "contact us "facility, for instance via its website or through electronic help desk for data subjects who want to:
 - (i) Enquire whether the organisation holds related personal information, or
 - (ii) Request access to related personal information, or

- (iii) Request the organisation to update or correct related personal information, or
- (iv) Make a complaint concerning the processing of personal information.

5.1.6. Security Safeguards

- a) NAMC will manage the security of its filing system to ensure that personal information is adequately protected. To this end, security controls will be implemented in order to minimise the risk of loss, unauthorised access, disclosure, interference, modification or destruction.
- b) Security measures also need to be applied in a context-sensitive manner. For example, the more sensitive the personal information, such as medical information or credit card details, the greater the security required.
- c) NAMC will continually review its security controls which will include regular testing of protocols and measures put in place to combat cyber-attacks on the organisation's IT network
- d) NAMC will ensure that all paper and electronic records comprising personal information are securely stored and made accessible to only authorised individuals.
- e) All new employees will be required to sign employment contracts containing contractual terms for the use and storage of employee information. Confidentiality clause will also be included to reduce the risk of unauthorised disclosures of personal information for which the organisation is responsible.
- f) All existing employees will, after the required consultation process has been followed, be required to sign an addendum to their employment containing the relevant consent and confidentiality clauses.
- g) NAMC's operators and third-party services will be required to enter into service level agreements with the organisation where both parties pledge with their mutual commitment to POPIA and the lawful processing of any personal information pursuant to the agreement. An example of "Employee Consent and Confidentiality Clause" for inclusion in NAMC's employment contracts can be found under **Annexure D**. An example of an "SLA Confidentiality Clause "for

inclusion in NAMC's service level agreements can be found under **Annexure E**.

5.1.7. Data subject participation

- a) A data subject may request the correction or deletion of his, or her personal information held by the organisation. NAMC will ensure that it provides a facility for data subjects who wants to request the correction of deletion of personal information. Where applicable, the organisation will include the link to unsubscribe from any of its electronic newsletter or related marketing activities.

6. INFORMATION OFFICERS

- 6.1. NAMC will appoint and Information Officer where necessary, a Deputy Information Officer to assist the Information Officer. NAMCs Information Officer is responsible for ensuring compliance with POPIA.
- 6.2. There are no legal requirements under POPIA for NAMC to appoint an Information Officer. Appointing an Information Officer is however, considered to be a good business practice, particularly within large organisations.
- 6.3. Where no Information Officer is appointed, the head of NAMC will assume the role of Information Officer. Consideration will be given on an annual basis to the re-appointment or replacement of an Information Officer and the re-appointment or replacement of any Deputy Information Officers.
- 6.4. Once appointed, NAMC will register the Information Officer with the South African Information Regulator established under POPIA prior to performing his or her duties. An example of an "Information Officer Appointment Letter" can be found under **Annexure F**.

7. SPECIFIC DUTIES AND RESPONSIBILITIES

7.1. Governing Body

- a) NAMC's governing body cannot delegate its accountability and its ultimately answerable for ensuring that the organisation meets its legal obligations in terms of POPIA. The governing body may however delegate some of its responsibilities in terms of POPIA to management or other capable individuals.

- b) The governing body is responsible for ensuring that:
 - (i) NAMC appoints an Information Officer and where necessary, a Deputy Information Officer. All persons responsible for the processing of personal information on behalf of the organisation: are appropriately trained and supervised to do so, understand that they are contractually obligated to protect the personal information they come into contact with, are aware that a wilful or negligent breach of this policy's processes and procedures may lead to disciplinary action being taken against them.

 - (ii) Data subjects who want to make enquiries about their personal information are made aware of the procedure that needs to be followed should they wish to do so.

 - (iii) The scheduling of a periodic POPIA audit in order to accurately assess and review the ways in which ARC collects, holds, uses, shares, discloses, destroys and processes personal information.

7.2. Information Officer

- a) NAMC's information Officer is responsible for:

- (iv) Taking steps to ensure NAMC's reasonable compliance with the provision of POPIA
- (v) Keeping the governing body updated about the organisation 's information protection responsible under POPIA. For instance, in the case of a security breach, the Information Officer must inform and advise governing body of their obligations pursuant to POPIA.
- (vi) Continually analysing privacy regulations and aligning them with the organisation 's personal information processing procedure. This will include reviewing NAMC's information protection procedures and related policies.
- (vii) Ensuring that POPIA Audits are scheduled and conducted on a regular basis.
- (viii) Ensuring that ARC makes it convenient for data subjects who want to update their personal information or submit POPIA related complaints to the organisation. For instance, maintaining a "contact us "facility on NAMC's website.
- (ix) Approving any contracts entered into with operators, employees and other third parties, which may have an impact on the personal information held by the organisation. This will include overseeing the amendment of NAMC's employment contracts and other service level agreements.
- (x) Encouraging compliance with the conditions required for the lawful processing of personal information.
- (xi) Ensuring that employees and other persons acting on behalf of NAMC are fully aware of the risk associated with the processing of personal information and that they remain informed about NAMC's security controls.
- (xii) Organising and overseeing the awareness training of employees and other individuals involved in the processing of personal information on behalf of NAMC.
- (xiii) Addressing employees' POPIA related questions.

- (xiv) Addressing all POPIA related requests and complaints made by NAMC's data subjects.
 - (xv) Working with the Information Regulator in relation to any ongoing investigations. The Information Officers will therefore act as the contact point of the Information Regulator authority on issues relating to the processing of personal information and will consult with the Information Regulator where appropriate, with regards to any other matter.
- b) The Deputy Information Officer will assist the Information Officer in performing his or her duties.

7.3. Employees and other persons acting on behalf of NAMC

- a) Employees and other persons acting on behalf of NAMC will, during the course of the performance of their services gain access to and become acquainted with the personal information of certain clients, suppliers and other employees.
- b) Employees and other persons acting on behalf of NAMC are required to treat personal information as a confidential business asset and to respect the privacy of data subjects.
- c) Employees and other persons acting on behalf of NAMC may not directly or indirectly, utilise, disclose or make public in any manner to any person or third party, either within NAMC or externally, any personal information, unless such information is already publicly known or the disclosure is necessary in order for the employee to perform his or her duty.
- d) Employees and other persons acting on behalf of NAMC may request assistance from their line manager or the Information Officer if they are unsure about any aspect related to the protection of a data subject's personal information.
- e) Employees and other persons acting on behalf of NAMC will only process personal information where:
 - (xvi) The data subject, or a competent person where the data subject is a child, consents to the processing; or

- (xvii) The processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party; or
 - (xviii) The processing complies with an obligation imposed by law on the responsible party; or
 - (xix) The processing protects a legitimate interest of the data subject; or
 - (xx) The processing is necessary for pursuing the legitimate interest of the organisation or of a third party to whom the information is supplied.
- f) Furthermore, personal information will only be processed where the data subject:
- (xxi) Clearly understands why and for what purpose his, or her personal information is been collected; and
 - (xxii) Has granted the organisation with explicit written or verbally recorded consent to process his, her or its personal information.
- g) Employee or persons acting on behalf of NAMC will consequently, prior to processing any personal information obtain a specific informed expression of will from the data subject, in terms of which permission is given for the processing of personal information.
- h) Informed consent is therefore when the data subject clearly understands for what purpose his, her or its personal information is needed and who it will be shared with. Consent can be obtained in written form, which includes any appropriate electronic medium that is accurately and readily reducible to printed form. Alternatively, NAMC will keep a voice recording of the data subject's consent in instances where transactions are concluded telephonically or via electronic video feed.
- i) Consent to process a data subject's personal information will be obtained directly from the data subject except where:
- (xxiii) the personal information has been made public, or
 - (xxiv) where valid consent has been given to a third party, or

- (xxv) the information is necessary for effective law enforcement.
- j) Employees or any other person acting on behalf of ARC will under no circumstances:
 - (xxvi) Process or have access to personal information where such processing or access is not requirement to perform their respective work-related task or duties.
 - (xxvii) Save copies of personal information directly to their own private computers, laptops or other mobile devices like tablets or smart phones. All personal information must be accessed and updated from the organisation's central database or dedicated server.
 - (xxviii) Share persona information informally. In particular, personal information should never be sent by email, as this form of communication is not secure. Where access to personal information is required, this may be requested from the relevant line manager or Information Officer.
 - (xxix) Transfer of personal information outside of South Africa without the express permission from the Information Officer.
- k) Employees and other persons acting on behalf of NAMC are responsible for:
 - (xxx) Keeping all personal information that they come into contact with secure, by taking precautions and following the guidelines outlined with this policy.
 - (xxxi) Ensuring that personal information is held in as few places as is necessary. No unnecessary additional records, filling system and data sets should therefore be created.
 - (xxxii) Ensuring that personal information is encrypted prior to sending or sharing the information electronically. The IT Manager will assist employees and where required, the other persons acting on behalf of the organisation, with the sending or sharing of personal information to or unauthorised external persons.

- (xxxiii) Ensuring that all computers, laptops and devices such as tablets, flash drives, and smart phones that store personal information are password protected and never left unattended. Passwords must be changed regularly and may not be shared with unauthorised persons.
- (xxxiv) Ensuring that their computer screens and other devices are switched off or locked when not in use or when away from their desk.
- (xxxv) Ensuring that where personal information is stored on removable storage medias such as external drives, CDs or DVDs that these are kept locked securely when not used.
- (xxxvi) Ensuring that where personal data is stored on paper, that such hard copy records are kept in a secure place where unauthorised person cannot access it. For instance, in a locked drawer of a filing cabinet.
- (xxxvii) Ensuring that where personal information has been printed out, that the paper printouts are not left unattended where unauthorised individuals could see or copy them. For instance, close to the printer.
- (xxxviii) Taking reasonable steps to ensure that personal information is kept accurate and up to date. For instance, confirming a data subject's details when the client or customer phones or communicate via email. Where a data subject's information is found to be out of date, authorisation must first be obtained from the relevant line manager or the Information Officer to update the information accordingly.
- (xxxix) Taking reasonable steps to ensure that personal information is stored only for as long as it is needed or required in terms of the purpose for what it was originally collected. Where personal information is no longer required, authorisation must first be obtained from the relevant line manager or Information Officer to delete or dispose of the personal information in the appropriate manner.
- (xl) Undergoing POPIA awareness training from time to time.

8. POPIA AUDIT

8.1. NAMC's Information Officer will schedule periodic POPIA Audits. The purpose of POPIA Audits is to:

- (xli) Identify the process used to collect, record, and store, disseminate and destroy personal information.
- (xlii) Redefine the purpose for gathering and processing personal information.
- (xliii) Ensure that the processing parameters are still adequately limited.
- (xliv) Ensure that new data subjects are made aware of the processing of their personal information.
- (xlv) Re-establish the rationale for any further processing where information is received via third party.
- (xlvi) Verify the quality of personal information.
- (xlvii) Monitor the extend of compliance with POPIA and this policy.
- (xlviii) Monitor the effectiveness of internal controls established to manage the organisation's POPIA related compliance risk.

8.2. In performing the POPIA Audit, Information Officers will liaise with the line manager in order to identify areas within in NAMC's operation that most valuable or susceptible to the unlawful processing of personal information. Information Officer will be permitted direct access to and have demonstrable support from Executive Management, line managers and the organisation's governing body in performing the audits.

9. REQUEST TO ACCESS PERSONAL INFORMATION

9.1. Data subjects have the rights to:

- (xlix) Request what personal information the organisation hold about them and why.
- (l) Request access to their personal information.
- (li) Be informed how to keep their personal information up to date.

9.2. Access to information requests can be made by email, addressed to the Information Officer. The Information Officers will provide the data subject with "Personal Information Request Form". Once the completed form has been received, the Information Officer will verify the identity of the data subject prior to handing over any personal information. All requests will be processed and considered against the organisation's PAIA Policy. The Information Officer will process requests within a reasonable time.

10. POPIA COMPLAINTS PROCEDURE

10.1. Data subjects have the rights to complain in instances where any of their rights under POPIA have been infringed upon. NAMC takes all complaints very seriously and will address all POPIA related complaints in accordance with the following procedure:

- (lii) POPIA complaints must be submitted to the organisation in writing. Where so required, the Information Officer will provide the data subject with a "POPIA Complaint Form".
- (liii) Where any person other than the Information Officer, that person, has received, the complaint will ensure that the full details of the complaint reach the Information Officer within 1 working day.
- (liv) The Information Officer will provide the complaint with a written acknowledgement of receipt of the complaint within 2 working days.
- (lv) The Information Officer will carefully consider the complaint and address the complaint's concerns in an amicable manner. In considering the complaint,

- the Information Officer will endeavour to resolve the complaint in a fair manner and in accordance with the principles outlined in POPIA.
- (lvi) The Information Officer must also determine whether the complaint relates to an error or breach of confidentiality that has occurred and which may have a wider impact on the organisation's data subjects.
 - (lvii) Where the Information Officer has a reason to believe that the personal information of data subject has been accessed or acquired by an unauthorised person, the Information Officer will consult with the organisation's governing body where after the affected data subjects and the Information Regulator will be informed of this breach.
 - (lviii) The Information Officer will revert to the complaint with a proposed solution with the option of escalating the complaints to the organisation's governing body within 7 working days of receipt of the complaint. In all instances, the organisation will provide reasons for any decisions taken and communicate any anticipated deviation from the specified timelines.
 - (lix) The information Officer's response the data subject may comprise any of the following:
 - a) A suggested remedy for the compliant,
 - b) A dismissal of the complaint and the reasons as to why it was dismissed,
 - c) An apology (if applicable) and any disciplinary action that has been taken against any employees involved.
 - (lx) Where data subject is not satisfied with the Information Officer's suggested remedies, the data subject has the right to complain to the Information Regulator.
 - (lxi) The Information Officer will review the complaints process to assess the effectiveness of the procedure on a periodic basis and to improve the procedure where it is found wanting. The reason for any complaint will also be reviewed to ensure the avoidance or occurrences giving rise to POPIA related complaints.

11. DISCIPLINARY ACTION

- 11.1. Where POPIA complaint or a POPIA infringement has been finalised, NAMC may recommend any appropriate administrative, legal and / or disciplinary action to be taken against any employee reasonably suspected of being implicated in any non-compliant activity outlined within this policy.
- 11.2. In the case of ignorance or minor negligence, NAMC will undertake to provide further awareness training to the employees.
- 11.3. Any gross negligence or wilful mismanagement of personal information will be considered a serious form of misconduct for which NAMC may summarily dismiss the employee. Disciplinary procedures will commence where there is sufficient evidence to support an employee's gross negligence.
- 11.4. Examples of immediate actions that may be taken subsequent to an investigation include:
 - (Ixii) A recommendation to commence with disciplinary action.
 - (Ixiii) A referral to appropriate law enforcement agencies for criminal investigation.
 - (Ixiv) Recovery of funds and assets in order to limit any prejudice or damage caused.

12. LEGISLATIVE FRAMEWORK

- 12.1. NAMC manages its legislative framework within its defined regulatory and legislative framework as defined within its Compliance Risk Management Framework.

13. REFERENCES

- 13.1. Compliance files, policies and mutual are maintained by the compliance functions. These includes:
 - (Ixv) Compliance Risk Management Framework

(Ixvi) Compliance Manual including all Policies, Processes and Procedures.

Request to any compliance information or documentation to be submitted to
POPIAcompliant@namc.co.za

14. APPROVAL STRUCTURES

14.1. Approval required by Council and Executive Management.

(Ixvii) POLICY SPONSOR

Chief Executive Officer

(Ixviii) Contact Person

The following person may be contacted in relation to this policy:

1. Information Officer

Dr Simphiwe Ngqangweni

Tel: 012 341 1115

Email: info@namc.co.za

2. Deputy Information Officer

Mr Stephen Monamodi

Tel: 012 341 1115

Majara@namc.co.za

ANNEXURE A:

PERSONAL INFORMATION REQUEST FORM

Please submit the completed form to the Information Officer	
Name	
Contact Number	
Email Address	

Please be aware that we may require you to provide proof of identification prior processing your request. There may also be a reasonable charge for providing copies of the information requested

A. Particulars of Data Subject	
Name & Surname:	
Identity Number:	
Postal Address:	
Contact Number:	
Email Address:	

B. Request

I request the organisation to:

- (a) Inform me whether it holds any of my personal information
- (b) Provide me with a record or description of my personal information
- (c) Correct or update my personal information
- (d) Destroy or delete a record of my personal information

C. Instructions

D. Signature Page

Signature

Date

ANNEXURE B: POPIA COMPLAINT FORM

We are committed to safeguarding your privacy and the confidentiality of your personal information and are bound by the Protection of Personal Information Act.

Please submit your complaint to the Information Officer	
Name	
Contact Number	
Email Address	

Where we are unable to resolve your complaint, to your satisfaction you have the right to complaint to the Information Regulator.

The Information Regulator:

Physical Address:

Email:

Website:

A. Particulars of Complaint	
Name & Surname:	
Identity Number:	
Postal Address:	
Contact Number:	
Email Address:	

D. Signature Page

Signature

Date

ANNEXURE C: POPIA NOTICE AND CONSENT FORM

We understand that your personal information is important to you and that you may be apprehensive about disclosing it. Your privacy is just as important to us and we are committed to safeguarding and processing your information in a lawful manner.

We also want to make sure that you understand how and for what purpose we process your information. If for any reason you think that your information is not processed in a correct manner, or that your information is being used for a purpose other than for what it was originally intended, you can contact our Information Officer.

You can request access to the information we hold about you at any time and if you think that we have outdated information, please request us to update or correct it.

Our Information Officer's contact details	
Name	
Contact Number	
Email Address	

Purpose for processing your information

We collect, hold, use and disclose your personal information mainly to provide you with access to the services and products that we provide. We will only process your information for a purpose you would reasonably expect, including:

14. Providing you with advice, products and services that suits your needs as requested
15. To verify your identity and to conduct credit reference searches.
16. To issue, administer and manage your insurance policies
- 17.

E. Particulars of Complaint	
Name & Surname:	
Identity Number:	
Postal Address:	
Contact Number:	
Email Address:	

F. Details of Complaint

G. Desired Outcome

H. Signature Page

Signature

Date

ANNEXURE D:

**REQUEST FOR ACCESS TO RECORD OF PUBLIC BODY
(Section 18(1) of the Promotion of Access to Information Act, 2000
(Act No. 2 of 2000)**

A. Particulars of public body

The Information Officer:

536 Francis Baard Street

Arcadia

0002

B. Particulars of person requesting access to the record

- (a) The particulars of the person who requests access to the record must be given below.
- (b) The address and/or fax number in the Republic to which the information is to be sent must be given.
- (c) Proof of the capacity in which the request is made, if applicable, must be attached.

Full names and surname:

Identity number:

Postal address:

Fax number:

Telephone number:

E-mail address:

Capacity in which request is made, when made on behalf of another person:

C. Particulars of person on whose behalf request is made

This section must be completed *ONLY* if a request for information is made on behalf of *another* person.

Full names and surname: _____

Identity number: _____

D. Particulars of record

- (a) Provide full particulars of the record to which access is requested, including the reference number if that is known to you, to enable the record to be located.
- (b) If the provided space is inadequate, please continue on a separate folio and attach it to this form.

The requester must sign all the additional folios.

1 Description of record or relevant part of the record:

2 Reference number, if available: _____

3 Any further particulars of record:

E. Fees

- (a) A request for access to a record, other *than* a record containing personal information about yourself, will be processed only after a request fee has been paid.
- (b) You will be *notified of* the amount required to be paid as the request fee.
- (c) The fee payable for access to a record depends *on* the form *in which* access is required and the reasonable time *required to* search for and prepare a record.
- (d) If you qualify for exemption *of* the payment *of* any fee, please state the reason for exemption.

Reason for exemption from payment of fees:

F. Form of access to record

If you are prevented by a disability to read, view or listen to the record in the form of access provided for in 1 to 4 hereunder, state your disability and indicate in which form the record is required.

Disability:	Form in which record is required:	Form in which record is required
-------------	-----------------------------------	----------------------------------

Mark the appropriate box with an X.

NOTES:

(a) Compliance with your request in the specified form may depend on the form in which the record is available.

(b) Access in the form requested may be refused in certain circumstances. In such a case you will be informed if access will be granted in another form.

(c) The fee payable for access for the record, if any, will be determined partly by the form in which access is requested.

1. If the record is in written or printed form:

	copy of record*		inspection of record
--	-----------------	--	----------------------

2. If record consists of visual images

this includes photographs, slides, video recordings, computer-generated images, sketches, etc)

	view the images		copy of the images"		transcription of the images*
--	-----------------	--	---------------------	--	------------------------------

3. If record consists of recorded words or information which can be reproduced in

sound:

	listen to the soundtrack audio cassette		transcription of soundtrack* written or printed document
--	--	--	---

4. If record is held on computer or in an electronic or machine-readable form:

	printed copy of record*		printed copy of information derived from the record"		copy in computer readable form* (stiffy or compact disc)
--	-------------------------	--	---	--	---

If you requested a copy or transcription of a record (above), do you wish the copy or transcription to be posted to you? Postage is payable.	YES	NO
---	-----	----

G Particulars of right to be exercised or protected

If the provided space is inadequate, please continue on a separate folio and attach it to this form. The requester must sign all the additional folios.

1. Indicate which right is to be exercised or protected:

2. Explain why the record requested is required for the exercise or protection of the aforementioned right:

H. Notice of decision regarding request for access

You will be notified in writing whether your request has been approved/denied. If you wish to be informed in another manner, please specify the manner and provide the necessary particulars to enable compliance with your request.

How would you prefer to be informed of the decision regarding your request for access to the record?

By email	<input type="checkbox"/>
By SMS	<input type="checkbox"/>
By telephone	<input type="checkbox"/>

Signed at..... This.....day of2021

**SIGNATURE OF REQUESTER / PERSON ON
WHOSE BEHALF REQUEST IS MADE**

ANNEXURE E:

OBJECTION TO THE PROCESSING OF PERSONAL INFORMATION IN TERMS OF SECTION 11(3) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013) REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018 [Regulation 2]

Note:

- 1. Affidavits or other documentary evidence as applicable in support of the objection may be attached.
- 2. If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.
- 3. Complete as is applicable.

Part A: DETAILS OF DATA SUBJECT

Name(s) and surname/ registered name of data subject:

Unique Identifier/ Identity Number

Residential, postal or business address:

Code ()

Contact number(s):

Fax number / E-mail address:

PART B DETAILS OF RESPONSIBLE PARTY

Name(s) and surname/ Registered name of responsible party:

Residential, postal or

Business address:

Code ()

Contact number(s):

Fax number/ E-mail address:

Part C REASONS FOR OBJECTION IN TERMS OF SECTION 11(1) (d) to (f)

(Please provide detailed reasons for the objection)

Signed at this day of2021

..... Signature of data subject/designated person

“Information Officer Appointment Letter” can be found under **Annexure F**