FAIS Ombud

PROTECTION OF PERSONAL INFORMATION POLICY

FAISOmbud Office of the Ombud for Financial Services Providers	**FAIS POPI POLICY** **VERSION 0.3**

Document name	FAIS Ombud POPIA Policy
Application	FAIS Ombud (FAIS Ombud)
For recommendation	Risk Committee
For approval	Ombud
Effective from	April 2023
To be reviewed	April 2025

NOTE:

A person using the FAIS Ombud documents or data must note the risk inherent in:

a) Distributing the documents or data without appropriate authorisation; and

b) Not using the documents or data as authorised or intended.

Document approval

Document owner

Name	Position
John Simpson	FAIS Ombud

20 June 2023

Document custodian

Name	Position
Karlien Hechter	GRC Officer

Document recommended by

Name	Position
Mr Hamilton Ratshefola	Chair of the Risk Committee

Version control and summary of changes

No.	Description Of Changes
0.1	First draft of the FAIS Ombud POPIA Policy
0.2	First draft reviewed for consideration by the Risk Committee and recommendation for approval by the Commissioner
0.3	2nd draft reviewed, updated FAIS Ombud particulars, no material changes.
0.4	Updated the policy to indicate the appointment of one Deputy Information Officer instead of two as per prior year.

Mandatory review period

To be reviewed every second year.

TABLE OF CONTENTS

GLOSSARY OF ABBREVIATIONS

EXCO	Executive Committee of the FAIS Ombud
FAIS Ombud	Ombud for Financial Services Providers
IT	Information Technology
NT	National Treasury
PAIA	Promotion of Access to Information (Act 4 of 2013)
PFMA	Public Finance Management Act (Act 1 of 1999, as amended)
POPIA	Protection of Personal Information Act

Note: THIS POLICY MUST BE READ IN CONJUNCTION WITH THE PAIA MANUAL

1. Introduction

The Office of the Ombud for Financial Services Providers ("FAIS Ombud") is a statutory body established in terms of Chapter VI of the Financial Advisory and Intermediary Services Act, Act No. 37 of 2002.

1.1 POPI Policy

The POPI Policy operationalise the POPI Act which gives effect to the constitutional right to privacy as set-out in Section 2 of the POPI Act.

The right to privacy is an integral human right recognised and protected in the South African Constitution and in the Protection of Personal Information Act 4 of 2013 ("POPIA"). POPIA aims to promote the protection of privacy by providing guiding principles that are intended to be applied to the processing of Personal Information in a context-sensitive manner. Through the provision of services, the Ombud Office is necessarily involved in the collection, use and disclosure of Personal Information of complainants, respondents, employees, service providers and other stakeholders.

A person's right to privacy entails having control over Personal Information and being able to conduct affairs relatively free from unwanted intrusions. Given the importance the constitutional right to privacy, the Ombud is committed to effectively manage Personal Information in its custody in accordance with the provisions of POPIA.

1.2 Purpose

The purpose of this policy is to protect the institution from the compliance risks associated with the protection of Personal Information which includes:

- Breaches of confidentiality. For instance, the institution could suffer penalties and/or possible litigation where it is found that the Personal Information of Data Subjects has been shared or disclosed inappropriately.
- The Office process personal information in terms of our statutory mandate as per the FSR Act and any other relevant legislation applicable to the institution.

- Reputational damage. For instance, the Office could suffer damage to its reputation following an adverse event such as a computer hacker illegally taking control over, threatening to steal, change, unlawfully share or destroy the Personal Information held by the Office.
- This policy demonstrates the Office's commitment to protecting the privacy rights of Data Subjects in the following manner:
  - Through stating desired behaviour and directing compliance with the provisions of POPIA and best practice.
  - By cultivating an organisational culture that recognises privacy as a valuable human right.
  - By developing and implementing internal controls for the purpose of managing the compliance risk associated with the protection of Personal Information.
  - By creating business practices that will provide reasonable assurance that the rights of Data Subjects are protected and balanced with the legitimate business needs of the Office.
  - By assigning specific duties and responsibilities to control owners, including the appointment of an Information Officer and where necessary, Deputy Information Officer, to protect the interests of the Office and Data Subjects.
  - By raising awareness through training and providing guidance to individuals who process Personal Information so that they can act confidently and consistently.

2. Sanctioning of policy

The Ombud or a delegated official of the FAIS Ombud is delegated by the Accounting Authority to act as custodian of this Policy. The full responsibility to ensure compliance with this Policy thereof lies with the Ombud or a delegated official.

No amendment shall be made to or any deviation undertaken from this Policy without the prior discussion thereof at the FAIS Ombud EXCO and written approval of the Accounting Authority or a delegated official. In the event of a need to deviate from any aspect of this Policy and procedures, a formal disposition document must be prepared stating the nature and the reasons for the proposed departure, presented to and discussed by the FAIS Ombud EXCO and submitted to the Accounting Authority or delegated official for approval.

The Policy shall be reviewed at least annually and it will be effective after the Accounting Authority has approved the amendments.

3. Definitions

3.1 Personal Information

Personal Information is any information that can be used to reveal a person's identity. Personal Information relates to an identifiable, living, natural person, and where applicable, an identifiable, existing juristic person (such as a Company), including, but not limited to information concerning—

- race, gender, sex, pregnancy, marital status, national or ethnic origin, colour, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language, and birth of a person;
- information relating to the education or the medical, financial, criminal or employment history of the person;
- any identifying number, symbol, email address, physical address, telephone number, location information, online identifier, or other particular assignment to the person;
- the biometric information of the person;
- the personal opinions, views, or preferences of the person;
- 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;
- the views or opinions of another individual about the person;
- 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.

3.2 Data Subject

This refers to the natural or juristic person to whom Personal Information relates, such as complainants, respondents, employees, service providers and other stakeholders or a company that supplies the Office with products or other goods.

3.3 Responsible Party

The Responsible Party is the entity that needs the Personal Information for a particular reason and determines the purpose of and means for processing the Personal Information. In this case, the Office is the Responsible Party.

3.4 Operator

An Operator means 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. For example, a third-party service provider that has contracted with the Office to shred documents containing Personal Information. When dealing with an Operator, it is considered good practice for a Responsible Party to include an indemnity clause.

3.5 Information Officer

The Information Officer is responsible for ensuring the Offices' compliance with POPIA. Where no Information Officer is appointed, the Ombud will be responsible for performing the Information Officer's duties.

Once appointed, the Information Officer must be registered with the South African Information Regulator established under POPIA prior to performing his or her duties. Deputy Information Officer can also be appointed to assist the Information Officer.

3.6 Processing

The act of processing information includes any activity or any set of operations, whether by automatic means, concerning Personal Information and includes—

- the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation, or use;
- dissemination by means of transmission, distribution or making available in any other form;
- merging, linking, as well as any restriction, degradation, erasure, or destruction of information.

3.7 Record

Means any recorded information, regardless of form or medium, including:

- Writing on any material;

- 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;
- Label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;
- Book, map, plan, graph, or drawing;
- Photograph, film, negative, tape or other device in which one or more visual images are embodied to be capable, with or without the aid of some other equipment, of being reproduced.

3.8 Filing System

Means any structured set of Personal Information, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria.

3.9 Unique Identifier

Means 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.

3.10 De-Identify

This means to delete any information that identifies a Data Subject, or which can be used by a reasonably foreseeable method to identify, or when linked to other information, that identifies the Data Subject.

3.11 Re-Identify

In relation to the Personal Information of a Data Subject, means to resurrect any information that has been de-identified that identifies the Data Subject, or can be used or manipulated by a reasonably foreseeable method to identify the Data Subject.

3.12 Consent

Means any voluntary, specific, and informed expression of will in terms of which permission is given for the processing of Personal Information.

3.13 Direct Marketing

Means to approach a Data Subject, either in person or by mail or electronic communication, for the direct or indirect purpose of—

- promoting or offering to supply, in the ordinary course of business, any goods or services to the Data Subject; or
- requesting the Data Subject to donate any kind for any reason.

3.14 Biometrics

Means a technique of personal identification that is based on physical, physiological, or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning, and voice recognition.

4. Policy Application

This policy and its guiding principles apply to:

- The Office's accounting authority;
- The Offices departments and business units;
- All employees and consultants, and
- All contractors, suppliers and other persons acting on behalf of the Office.

The policy's guiding principles find application in all situations and must be read in conjunction with POPIA as well as the Office's PAIA Policy as required by the Promotion of Access to Information Act (Act No 2 of 2000).

The legal duty to comply with POPIA's provisions is activated in any situation where there is a processing of Personal Information by or for a Responsible Party who is domiciled in South Africa.

POPIA does not apply in situations where the processing of Personal Information—

- is concluded during purely personal or household activities, or
- where the Personal Information has been de-identified.

5. Rights of Data Subjects

Where appropriate, the Office will ensure that its complainants, respondents, employees, service providers and other stakeholders are made aware of the rights conferred upon them as Data Subjects.

The Office will ensure that it gives effect to the following six rights.

5.1 The Right to Access Personal Information

The Office recognises that a Data Subject has the right to establish whether the Office holds Personal Information related to him, her, or it, including the right to request access to that Personal Information.

5.2 The Right to have Personal Information Corrected or Deleted

The Data Subject has the right to request, where necessary, that his, her or its Personal Information must be corrected or deleted where the Office is no longer authorised to retain the Personal Information.

5.3 The Right to Object to the Processing of Personal Information

The Data Subject has the right, on reasonable grounds, to object to the processing of his, her or its Personal Information. In such circumstances, the Office will give due consideration to the request and the requirements of POPIA. The Office 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 the Personal Information.

5.4 The Right to Object to Direct Marketing

The Data Subject has the right to object to the processing of his, her or its Personal Information for purposes of direct marketing by means of unsolicited electronic communications.

5.5 The Right to Complain to the Information Regulator

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.

5.6 The Right to be Informed

The Data Subject has the right to be notified that his, her or its Personal Information is being collected by the Office. The Data Subject also has the right to be notified in any situation where the organisation has reasonable grounds to believe that the Personal Information of the Data Subject has been accessed or acquired by an unauthorised person.

6. General guiding principles

All respondents, employees, service providers and other stakeholders acting on behalf of the Office will always be subject to, and act in accordance with, the following guiding principles:

6.1 Accountability

Failing to comply with POPIA could potentially damage the Office reputation or expose the Office to a civil claim for damages. The protection of Personal Information is therefore everybody's responsibility.

The Office will ensure that the provisions of POPIA and the guiding principles outlined in this policy are complied with through the encouragement of desired behaviour. However, the Office will take appropriate sanctions, which may include disciplinary action, against those individuals who, through their intentional or negligent actions and/or omissions, fail to comply with the principles and responsibilities outlined in this policy.

6.2 Processing Limitation

The Office will ensure that Personal Information under its control is processed:

- in a fair, lawful, and non-excessive manner, and
- only with the informed consent of the Data Subject, and
- only for a specifically defined purpose.

The Office 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. Alternatively, where services or transactions are concluded over the telephone or electronic video feed, the Office will maintain a voice recording of the stated purpose for collecting the Personal Information followed by the Data Subject's subsequent consent.

The Office 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.

Where applicable, the Data Subject must be informed of the possibility that their Personal Information will be shared with other aspects of the Office's business and be provided with the reasons for doing so.

6.3 Purpose Specification

All the Office's departments and business units a must be informed by the principle of transparency. The Office will process Personal Information only for specific, explicitly defined and legitimate reasons. The Office will inform Data Subjects of these reasons prior to collecting or recording the Data Subject's Personal Information.

6.4 Further Processing Limitation

Personal Information will not be processed for a secondary purpose unless that processing is compatible with the original purpose. Therefore, where the Office 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, the Office will first obtain additional consent from the Data Subject.

6.5 Information Quality

The Office will take reasonable steps to ensure that all Personal Information collected is complete, accurate and not misleading. The more important it is for the Personal Information to be accurate (for example, the beneficiary details of a life insurance policy are of the utmost

importance), the greater the effort the Office will put into ensuring its accuracy. Where Personal Information is collected or received from third parties, the Office 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.

6.6 Open Communication

The Office will take reasonable steps to ensure that Data Subjects are notified (are always aware) that their Personal Information is being collected including the purpose for which it is being collected and processed.

The Office will ensure that it establishes and maintains a “contact us” facility, for instance via its website or through an electronic helpdesk, for Data Subjects who want to—

- enquire whether the Office holds related Personal Information, or
- request access to related Personal Information, or
- request the Office to update or correct related Personal Information, or
- make a complaint concerning the processing of Personal Information.

6.7 Security Safeguards

The Office will manage the security of its filing / data record-keeping system to ensure that Personal Information is adequately protected. To this end, security controls will be implemented to minimise the risk of loss, unauthorised access, disclosure, interference, modification, or destruction.

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.

The Office will continuously review its security controls which will include regular testing of protocols and measures put in place to combat cyber-attacks on the Office’s IT network. The Office will ensure that all paper and electronic records comprising Personal Information are securely stored and made accessible only to authorised individuals.

All new employees will be required to sign employment contracts containing contractual terms for the use and storage of employee information. Confidentiality clauses will also be included to

reduce the risk of unauthorised disclosures of Personal Information for which the Office is responsible.

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.

The Office'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.

6.8 Data Subject Participation

A Data Subject may request the correction or deletion of his, her or its Personal Information held by the Office. The Office will ensure that it provides a facility for Data Subjects who want to request the correction of deletion of their Personal Information. Where applicable, the Office will include a link to unsubscribe from any of its electronic newsletters or related marketing activities.

7. Information Officers

The Office has appointed an Information Officer and one Deputy Information Officer to assist the Information Officer. The Office's Information Officer is responsible for ensuring compliance with POPIA.

Consideration will be given on an annual basis to the re-appointment or replacement of the Deputy Information Officer and the re-appointment or replacement of new Deputy Information Officers. Once appointed, the Office will register the Information Officer and the Deputies with the South African Information Regulator established under POPIA prior to performing his or her duties.

8. Specific Duties and Responsibilities

8.1 Accounting Authority

The Office's Accounting Authority cannot delegate its accountability and is ultimately answerable for Accounting Authority may however delegate some of its responsibilities in terms of POPIA to management or other capable individuals.

The Accounting Authority is responsible for ensuring that:

- The Office appointed an Information Officer, and one Deputy Information Officer;
- All persons responsible for the processing of Personal Information on behalf of the Office—
  - are appropriately trained and supervised to do so;
  - understand that they are contractually obligated to protect the Personal Information they meet, and
  - are aware that a wilful or negligent breach of this policy's processes and procedures may lead to disciplinary action being taken against them.
- 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;
- Periodic POPI Audits are scheduled to accurately assess and review the ways in which the Office collects, holds, uses, shares, discloses, destroys, and processes Personal Information.

8.2 Information Officer

The Office's Information Officer is responsible for:

- Taking steps to ensure the Office's reasonable compliance with the provision of POPIA;
- Keeping the accounting authority updated about the Office's information protection responsibilities under POPIA. For instance, in the case of a security breach, the Information Officer must inform and advise the accounting authority of their obligations pursuant to POPIA;
- Continually analysing privacy regulations and aligning them with the Office's Personal Information processing procedures. This will include reviewing the Office's information protection procedures and related policies;
- Ensuring that POPI Audits are scheduled and conducted on a regular basis;
- Ensuring that the Office makes it convenient for Data Subjects who want to update their Personal Information or submit POPIA related complaints to the Office. For instance, maintaining a "contact us" facility on the Office's website;

- Approving any contracts entered with Operators, employees and other third parties which may have an impact on the Personal Information held by the Office . This will include overseeing the amendment of the Office's employment contracts and other service level agreements.
- Encouraging compliance with the conditions required for the lawful processing of Personal Information;
- Ensuring that employees and other persons acting on behalf of the Office are fully aware of the risks associated with the processing of Personal Information, and that they remain informed about the Office's security controls;
- Oversee and ensure the organisation of awareness training of employees and other individuals involved in the processing of Personal Information on behalf of the Office;
- Addressing employees' POPIA related questions;
- Addressing all POPIA related requests/complaints made by the Office's Data Subjects;
- Working with the Information Regulator in relation to any ongoing investigations. The Information Officers will therefore act as the contact point for the Information Regulator authority on issues relating to the processing of Personal Information and will consult with the Information Regulator where appropriate, with regard to any other matter. The Deputy Information Officer will assist the Information Officer in performing his duties.

8.3 IT Manager

The Office's IT Manager is responsible for:

- Ensuring that the Office's IT infrastructure, filing systems and any other devices used for processing Personal Information meet acceptable security standards;
- Ensuring that all electronically held Personal Information is kept only on designated drives and servers and uploaded only to approved cloud computing services;
- Ensuring that servers containing Personal Information are sited in a secure location, away from the general office space;
- Ensuring that all electronically stored Personal Information is backed-up and tested on a regular basis;

- Ensuring that all back-ups containing Personal Information are protected from unauthorised access, accidental deletion and malicious hacking attempts;
- Ensuring that Personal Information being transferred electronically is encrypted;
- Ensuring that all servers and computers containing Personal Information are protected by a firewall and the latest security software;
- Performing regular IT audits to ensure that the security of the Office's hardware and software systems are functioning properly;
- Performing regular IT audits to verify whether electronically stored Personal Information has been accessed or acquired by any unauthorised persons;
- Performing a proper due diligence review prior to contracting with service providers s to process Personal Information on the Office's behalf. For instance, cloud computing services.

8.4 Marketing & Communication Practitioner

The Office's Marketing & Communication Practitioner is responsible for:

- Approving and maintaining the protection of Personal Information statements and disclaimers that are displayed on the Office's website, including those attached to communications such as emails and electronic newsletters;
- Addressing any Personal Information protection queries from journalists or media outlets such as newspapers;
- Where necessary, working with persons acting on behalf of the Office to ensure that any outsourced marketing initiatives comply with POPIA.

8.5 Employees and other Persons acting on behalf of the Office

Employees, service providers and any other stakeholders acting on behalf of the Office will, during the performance of their services, gain access to and become acquainted with the Personal Information of certain complainants, respondents, employees, service providers and other stakeholders.

Employees, service providers and any other stakeholders acting on behalf of the Office are required to treat Personal Information as a confidential business asset and to respect the privacy of Data Subjects.

Employees, service providers and any other stakeholders acting of the Office may not directly or indirectly, utilise, disclose, or make public in any manner to any person or third party, either within the Office or externally, any Personal Information, unless such information is already publicly known, or the disclosure is necessary in order for the employee or person to perform his or her duties.

Employees, service providers and any other stakeholders acting on behalf of the Office must request assistance from their line manager or the Information Officer/Deputy Information Officer if they are unsure about any aspect related to the protection of a Data Subject's Personal Information.

Employees, service providers and any other stakeholders acting on behalf of the Office will only process Personal Information where:

- The Data Subject, or a competent person where the Data Subject is a child, consents to the processing; or
- 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
- The processing complies with an obligation imposed by law on the Responsible Party; or
- The processing protects a legitimate interest of the Data Subject; or
- The processing is necessary for pursuing the legitimate interests of the Office or of a third party to whom the information is supplied.
- Furthermore, Personal Information will only be processed where the Data Subject:
- Clearly understands why and for what purpose his, her or its Personal Information is being collected; and
- Has granted the Office with explicit written or verbally recorded consent to process his, her or its Personal Information.

Employees, service providers and any other stakeholders acting on behalf of the Office will consequently, prior to processing any Personal Information, obtain a specific and informed expression of will from the Data Subject, in terms of which permission is given for the processing of Personal Information. 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, the Office will keep a voice recording of the Data Subject's consent in instances where transactions are concluded telephonically or via electronic video feed.

Consent to process a Data Subject's Personal Information will be obtained directly from the Data Subject, except where—

- the Personal Information has been made public, or
- where valid consent has been given to a third party, or
- the information is necessary for effective law enforcement.

Employees, service providers and any other stakeholders acting on behalf of the Office will under no circumstances:

- Process or have access to Personal Information where such processing or access is not a requirement to perform their respective work-related tasks or duties;
- 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 Office's central database or a dedicated server;
- Employees and other persons acting on behalf of the Office are responsible for—
  - keeping all Personal Information that they come into contact with secure, by taking sensible precautions and following the guidelines outlined within this policy;
  - ensuring that Personal Information is held in as few places as is necessary. No unnecessary additional records, filing systems and data sets should therefore be created;
  - ensuring that Personal Information is encrypted prior to sending or sharing the information electronically. The IT Manager will assist employees and where required, other persons acting on behalf of the Office, with the sending or sharing of Personal Information to or with authorised external persons;
  - ensuring that all computers, laptops, and devices such as tablets, flash drives and smartphones that store Personal Information are password protected and never left unattended. Passwords must be changed regularly and may not be shared with unauthorised persons;

- ensuring that their computer screens and other devices are switched off or locked when not in use or when away from their desks;
- ensuring that where Personal Information is stored on removable storage medias e.g., external drives/CDs/DVDs that these are kept locked away securely when not in use;
- ensuring that where Personal Information is stored on paper, that such hard copy records are kept in a secure place where unauthorised people cannot access it. For instance, in a locked drawer of a filing cabinet;
- 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;
- taking reasonable steps to ensure that Personal Information is kept accurate and up to date. For instance, confirming a Data Subject's contact details when the client or customer phones or communicates 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/Deputy Information Officer to update the information accordingly;
- 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 which it was originally collected. Where Personal Information is no longer required, authorisation must first be obtained from the relevant line manager or the Information Officer/Deputy information Officer to delete or dispose of the Personal Information in the appropriate manner;
- undergoing POPI Awareness training from time to time.

Where an employee, service providers and any other stakeholders acting on behalf of the Office, 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/Deputy Information Officer.

9. POPI Audit

The Office's Information Officer will schedule periodic POPI Audits. The purpose of a POPI audit is to:

- Identify the processes used to collect, record, store, disseminate and destroy Personal Information;
- Determine the flow of Personal Information throughout the Office. For instance, the Office's various departments;
- Ensure that the processing parameters are still adequately limited;
- Ensure that new Data Subjects are made aware of the processing of their Personal Information;
- Re-establish the rationale for any further processing where information is received via a third party;
- Verify the quality and security of Personal Information;
- Monitor the extent of compliance with POPIA and this policy;
- Monitor the effectiveness of internal controls established to manage the Office's 's POPI related compliance risk.

In performing the POPI Audit, Information Officers will liaise with line managers in order to identify areas within in the Office's operation that are most vulnerable or susceptible to the unlawful processing of Personal Information. Information Officers will be permitted direct access to and have demonstrable support from line managers and the Office's accounting authority in performing their duties.

10. Request to access personal information procedure

Data Subjects have the right to:

- Request what Personal Information the Office holds about them and why;
- Request access to their Personal Information, and
- Be informed how to keep their Personal Information up to date.

Access to information requests can be made by email, addressed to the Information Officer/Deputy Information Officer. The Information Officer/Deputy Information Officer will provide the Data Subject with a "Personal Information Request Form".

Once the completed form has been received, the Information Officer/Deputy 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 Office's PAIA Manual. The Information Officer/Deputy Information Officer will process all requests within a reasonable time.

11. POPI Complaints Procedure

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

- POPI complaints must be submitted to the Office in writing. Where so required, the Information Officer/Deputy Information Officer will provide the Data Subject with an "OBJECTION TO THE PROCESSING OF PERSONAL INFORMATION IN TERMS OF SECTION 11(3) OF POPIA Form" – refer to PAIA Manual, Annexure 4.
- Where the complaint has been received by any person other than the Information Officer/Deputy Information Officer, that person will ensure that the full details of the complaint reach the Information Officer within 3 working days;
- The Information Officer/Deputy Information Officer will provide the complainant with a written acknowledgement of receipt of the complaint within 2 working days;
- The Information Officer/Deputy Information Officer will carefully consider the complaint and address the complainant's concerns in an amicable manner. In considering the complaint, the Information Officer/Deputy Information Officer will endeavour to resolve the complaint in a fair manner and in accordance with the principles outlined in POPIA;
- The Information Officer/Deputy 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 Company's Data Subjects;
- Where the Information Officer/Deputy Information Officer has reason to believe that the Personal Information of Data Subjects has been accessed or acquired by an unauthorised person, the Information Officer will consult with the Office's accounting authority where after the affected Data Subjects and the Information Regulator will be informed of this breach;

- The Information Officer/Deputy Information Officer will revert to the complainant with a proposed solution with the option of escalating the complaint to the Office's accounting authority within 7 working days of receipt of the complaint. In all instances, the Office will provide reasons for any decisions taken and communicate any anticipated deviation from the specified timelines;
- The Information Officer's/Deputy Information Officer response to the Data Subject may comprise any of the following:
  - A suggested remedy for the complaint;
  - A dismissal of the complaint and the reasons as to why it was dismissed;
  - An apology (if applicable) and any disciplinary action that has been taken against any employees involved.
- Where the Data Subject is not satisfied with the Information Officer's/Deputy Information Officer suggested remedies, the Data Subject has the right to complain to the Information Regulator.
- The Information Officer/Deputy 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 complaints will also be reviewed to ensure the avoidance of occurrences giving rise to POPI related complaints.

12. Disciplinary Action

Where a POPI complaint or a POPI infringement investigation has been finalised, the Office 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.

In the case of ignorance or minor negligence, the Office will undertake to provide further awareness training to the employee. Any gross negligence or the wilful mismanagement of Personal Information, will be considered a serious form of misconduct for which the Office may summarily dismiss the employee. Disciplinary procedures will commence where there is sufficient evidence to support an employee's gross negligence.

Examples of immediate actions that may be taken after an investigation include:

- A recommendation to commence with disciplinary action;

- A referral to appropriate law enforcement agencies for criminal investigation;
- Recovery of funds and assets to limit any prejudice or damages caused.