WORLDWIDE ADVISORY SERVICES (PTY) LTD

(Hereinafter referred to as 'the Company/WWAS')

PROTECTION OF PERSONAL INFORMATION FRAMEWORK AND PRIVACY POLICY

In terms of the
Protection of Personal Information Act 4 of 2013 ("PoPIA")

Worldwide
Advisory Services

Contents

DOCUMENT MANAGEMENT
Title: WWAS Protection of Personal Information Framework and Privacy Policy
Implementation Date: July 2022
Version Status: 1.03
Last Review Date: August 2025
Next Review Date: August 2026 or in the event of a material legislative change

VERSION AND APPROVAL CONTROL				
Version	**Type**	**Summary of actions/changes**	**Responsible Party**	**Date**
V 1.0	New	New document produced	Byron Bosch (Legal & Compliance)	July 2022
V 1.0	Approval	Approved	Tyrone Waterston (Key Individual)	August 2022
V 1.01	Revised & approved	Approval required (KI)	Byron Bosch (Legal & Compliance) Tyrone Waterston (Key Individual)	August 2023
V 1.02	Revised & approved	Approval required (KI)	Byron Bosch (Legal & Compliance) Tyrone Waterston (Key Individual)	August 2024
V 1.03	Revised & approved	Approval required (KI)	Byron Bosch (Legal & Compliance) Tyrone Waterston (Key Individual)	August 2025

VERSION TYPE

□ New/Draft/Replacement □ Amendment □ Review (Annual/Ad Hoc) √ Approved

1. Introduction

The Protection of Personal Information Act 4 of 2013 (PoPIA/The Act), and the Regulations promulgated thereunder, give effect to the right to privacy, provided by Section 14 of the Bill of Rights of the Constitution of the Republic of South Africa 1996.

The Act and Regulations require a Responsible Party to appoint an Information Officer, in terms of the Promotion of Access to Information Act 2 of 2000 (PAIA), to develop, implement, monitor, and maintain a compliance PoPIA Framework and Privacy Policy.

The FSP, in its capacity as a Responsible Party, has developed this PoPIA Framework and Privacy Policy in order to comply with the aforesaid requirements and to further demonstrate commitment to the Act, Data Subjects and the processing of Personal Information.

The FSP must ensure that an Information Officer and any applicable Deputy Information Officer(s) are registered with the Information Regulator.

2. Purpose

The purpose of the PoPIA is to give effect to the constitutional right to privacy. This is achieved by safeguarding Personal Information when processed by a Responsible Party, subject to justifiable limitations that are aimed at balancing the right to privacy against other rights, particularly the right of access to information; and protecting important interests, including the free flow of information within the Republic of South Africa and across international borders.

The Act regulates 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. Furthermore, it provides persons with rights and remedies to protect their Personal Information from processing that is not in accordance with the Act.

3. Scope and Application

This PoPIA Framework and Privacy Policy applies to all employees of the FSP and anyone who may process Personal Information for and on behalf of the FSP.

Furthermore, it applies to all situations and business processes where Personal Information is processed, more importantly where such information may be made accessible to third parties. This PoPIA Framework and Privacy Policy must be read together with the FSP's PAIA Manual.

4. Definitions

Applicable Legislation means all legislation applicable to the FSP, as specified in the FSP's PAIA Manual, under the heading "Records available in terms of other Legislation".

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.

Consent means any voluntary, specific, and informed expression of will in terms of which permission is given for the processing of personal information.

Data subject refers to the natural or juristic persons to whom personal information relates.

De-identify 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.

Direct Marketing means to approach a Data Subject, either in person, 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 make a donation of any kind for any reason.

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.

Employee means, for the purposes of this PoPIA Framework and Privacy Policy, any person employed permanently (full- or part-time), temporary, or on a fixed-term contract, and includes Key Individual's, Representatives, Juristic Representatives, and contractors that may come into contact with, use, process or otherwise deal with Personal Information.

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.

Office-bearer means the members of the Board, the Principal Officer, members of Committees, governance secretaries and persons in similar positions.

Information Officer means the head of the private body as contemplated in Section 1 of the Promotion of Access to Information Act 2000 and who has been registered with the Information Regulator in such capacity.

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.

Person means a natural or juristic person.

Personal Information shall mean, for purposes of this PoPIA Framework and Privacy Policy and as defined under the Act, information about an identifiable, natural person, and in so far as it is applicable, an identifiable, juristic person, including, but not limited to:

- 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;
- information relating to the education or the medical, criminal or employment history of the person or information relating to financial transactions in which the person has been involved;
- any identifying number, symbol or other particular assigned to the person;
- the address, fingerprints or blood type of the person;
- the personal opinions, views or preferences of the person, except where they are about another individual or about a proposal for a grant, an award of a prize to be made to another individual;
- 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 views or opinions of another individual about a proposal for a grant, an award, or a prize to be made to the person, but excluding the name of the other individual where it appears with the views or opinions of the other individual; and
- the name of the person where it appears with other personal information relating to the person or where the disclosure of the name itself would reveal information about the person;
- but excludes information about a natural person who has been dead, or a juristic person that has ceased to exist, for more than 20 years.

PoPIA Framework and Privacy Policy means this PoPIA Framework and Privacy Policy developed in terms of the Act and Regulations thereto;

Processing means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including:

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

Purpose means the FSP's purpose when processing of Personal Information as set out under the FSP's PAIA Manual as well as on the Notice and Consent Form;

Record means any recorded information:-

- regardless of form or medium, including any of the following:
  - 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 so as to be capable, with or without the aid of some other equipment, of being reproduced;
- in the possession or under the control of a responsible party;
- whether or not it was created by a responsible party; and
- regardless of when it came into existence.

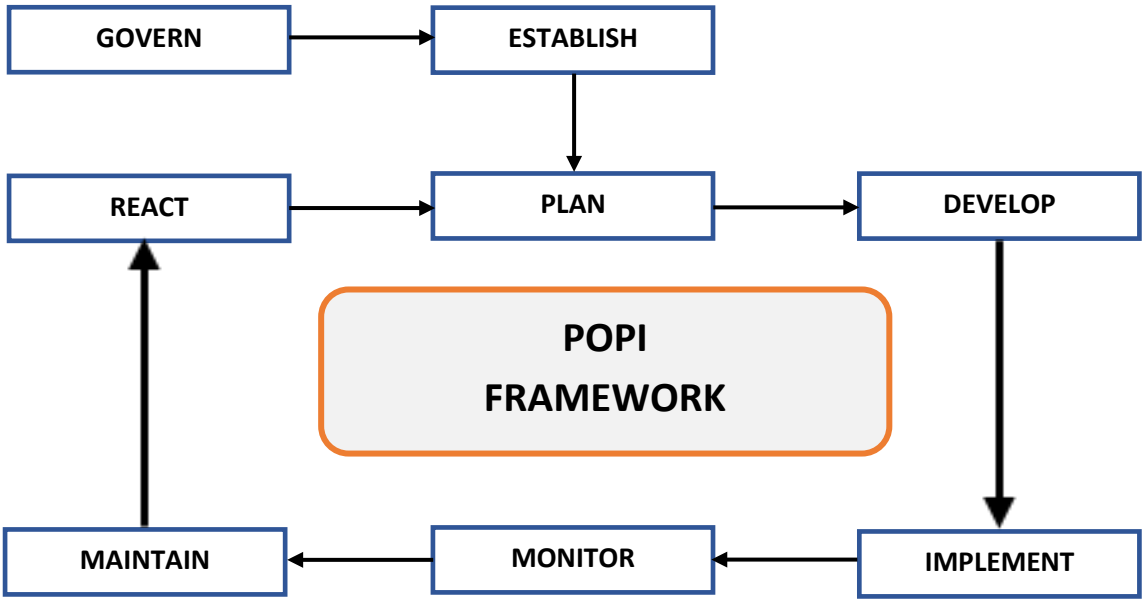
Re-identify in relation to personal information of a Data Subject, means to resurrect any information that has been de-identified that identifies the Data Subject, or can be used or manipulated by a reasonably foreseeable method to identify the Data Subject.

Responsible Party means, for purposes of this PoPIA Framework and Privacy Policy, all persons to whom this PoPIA Framework and Privacy Policy applies, whom, whether alone or in conjunction with others determines the purpose and means of processing Personal Information.

Special Personal Information means information relating to a person's (a) religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a Data Subject; or (b) criminal behavior, as defined under the Act.

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.

5. The Basis of our PoPIA Compliance Framework



Govern

Governance is best described as the system by which entities are directed and controlled. It is concerned with structure and processes for decision making, accountability, control, and behaviour at the top of an entity. Governance influences how the FSP's objectives are set and achieved, how risk is monitored and addressed and how performance is optimised. Governance is a system and process, not a single activity, therefore, successful implementation of a good governance strategy requires a systematic approach that incorporates strategic planning, risk management, and performance management. Like culture, it is a core component of the unique characteristics of a successful organisation.

Establish and conclude a formal impact assessment

The Act requires a formal Impact Assessment to be conducted in order to establish the needs and objectives of the business in relation to PoPIA risk planning.

Plan

Following the results from the Impact Assessment, the FSP will analyse, plan, and strategise its data flow and security measures to ensure that it can minimise, mitigate, or eliminate risks posed to the FSP. A Risk Management Plan is required to manage risks and will also help establish what compliance will look like and, most importantly, how to control and minimise risks.

Develop

The FSP must develop policies, procedures, and process in line with the requirements of PoPIA as well as the nature and scale of its business activities. The compliance PoPIA Framework and Privacy Policy will prove futile if the FSP does not have the correct documentation in place to guide, protect, and entrench PoPIA within it.

The FSP must ensure that it has the right policies, guidelines, contracts, and clauses in place to manage risk and liability.

Implement

The first step to implementation is to manage expectations by ensuring that all persons within the FSP are on the same page and understand the documentation, the implementation procedure, and what to expect from the process. The following elements are essential to the FSP's PoPIA implementation:

Direct involvement of senior persons in the process and understanding that active participation throughout the FSP is necessary:

- Once external support structures step back, senior persons within the FSP need to be willing and able to carry the process forward.

Awareness that despite all the measures put in place, the most significant risk of a breach or non-compliance remains the human staff:

- A clear understanding of key terms and concepts across the entire FSP is essential. The risk of an ill-informed workforce is real and may render the whole compliance process futile.
- Ensure adequate and regular training of all individuals within the FSP. This should cover what individuals may and may not do with personal information and what the internal policies actually are.
- Differentiated training within the FSP, depending on the type and level of access individuals have to personal information, is essential.
- Ensure internal systems contain disciplinary measures and communicate the consequences clearly.

A clear understanding that PoPIA processes do not have a specified end:

- It is an indefinite, ongoing process that needs to become entrenched in the day-to-day operations of the FSP. It is not a once off process but requires consistent review and analysis.

Monitor and audit

Once the PoPIA Framework and Privacy Policy is operational, the FSP will be able to identify gaps or further risks. It is common for unforeseen and unexpected compliance issues to arise even a year or more after implementation plans have concluded. For this reason, it is imperative that the FSP constantly monitors its processes and procedures.

The Information Officer will schedule periodic PoPIA Audits to:

- Identify the processes used to collect, record, store, disseminate, and destroy personal information.
- Determine the flow of personal information throughout the FSP and its various business units', divisions, and/or branches.
- Redefine the purpose for gathering and processing personal information.
- Ensure that the processing parameters are still adequately limited.
- 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 Framework and Privacy Policy.
- Monitor the effectiveness of internal controls established to manage the organisation's PoPIA related compliance risk.

In performing the PoPIA Audit, the Information Officer will liaise with line managers to identify areas that are most vulnerable or susceptible to the unlawful processing of personal information. The Information Officer will have direct access to and have demonstrable support from line managers and the FSP's governing body in performing his/her duties.

Maintain

It is important to ensure that processes and procedures that are put in place are maintained and updated due to the changing needs of the FSP, its clients and the regulatory landscape.

React

It is vitally important for the FSP to have procedures in place when reacting to disaster situations. Disaster management plans ensures that the FSP plans ahead and develops protocols to address the disaster, safeguard its reputation, and minimise the recovery time following the occurrence of the disaster. It also involves detailing the FSP's response to non-compliance or contraventions of the PoPIA.

6. The FSP Requirements for Processing Personal Information

All Processing of Personal Information must only be effected after the Data Subject has provided express consent and has signed with the FSP's approved PoPIA Notice and Consent Form (Annexure A).

Where there is a legal requirement to disclose Personal Information to authorities, and consent is not required by law, the Data Subject must still be notified of such disclosure, unless the Applicable Law provides otherwise.

7. Notifications

The FSP will provide notification to all persons whose information is being processed. This is done via the FSP's PoPIA Notice and Consent Form (Annexure A), Website Privacy Notice, Website Disclaimer and Terms and Conditions, specific consents to disclosure, and, where bulk-mailers or communications are sent out, with a statement relating to the rights of the Data Subject, attached thereto.

The Data Subject has the right to:

- Be notified when personal information is being collected, the type of information collected, for what purpose, whether the information is to be supplied voluntarily or is collected mandatory, and whether the information would be transferred to a third country and the protections afforded there;
- Be notified when there has been unlawful access or acquisition of personal information;
- Request a record of their Personal Information;
- Request the correction, deletion and/or destruction of their Personal Information;
- Object to the processing of their Personal Information;
- Exercise the right to withdraw the consent to processing, if voluntarily given;
- Not be subjected to unsolicited electronic communication, unless he/she/it is a customer and the FSP has provided services to him/her/it, or where the Data Subject has consented to the communication and had the opportunity to object to the communication;
- Not to be subjected to automated decision-making based on the personal information in contravention of Section 71, PoPIA;

- Submit a complaint to the Information Regulator at www.justice.gov.za/inforeg/index.html; and
- Institute civil proceedings regarding an alleged interference with his/her/its personal information in terms of Section 99, PoPIA.
- Be provided with the details of the Information Officer, or the responsible Deputy Information Officer.

8. Conditions of Lawful Processing of Personal Information

Section 4(1) of the Act requires that all Processing of Personal Information be done in a lawful manner. Any person who processes Personal Information for and on behalf the FSP must do so in terms of the below conditions in order to ensure compliance with the Act.

Condition 1: Accountability

- Ensure that all the conditions and measures giving effect to conditions of the lawful processing of Personal Information, as set out in the Act and this PoPIA Framework and Privacy Policy, are complied with at the time of determining the purpose and means of processing and during the processing.
- Failing to comply with PoPIA could potentially damage the FSP's reputation or expose it to a civil claim for damages.
- The FSP 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.
- The FSP's governing body cannot delegate its accountability and is ultimately answerable for ensuring that the FSP 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.
- The governing body is responsible for ensuring that:
  - The FSP appoints an Information Officer, and where necessary, a Deputy Information Officer.
  - All persons responsible for the processing of personal information on behalf of the FSP:
    Are appropriately trained and supervised to do so;
    Understand that they are contractually obligated to protect the personal information they come into contact with; and
    Are aware that a willful 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.
- The scheduling of a periodic PoPIA Audit, in order to accurately assess and review the ways in which the FSP collects, holds, uses, shares, discloses, destroys, and processes personal information.

Condition 2: Processing Limitation

- Personal Information must only be processed with the consent of the Data Subject, for a specific, explicit, and lawfully defined purpose, related to the functions and activities of the FSP, or if under a statutory obligation, with a notification to the person of the specific statutory reference or citation.

- The FSP will ensure that Personal Information under its control is processed in a fair, lawful, and non-excessive manner, and only for a specifically defined purpose.
- All consents to processing and/or notifications of processing will be reviewed by responsible employees to ensure that it is specific. In cases of uncertainty, the Information Officer or one of his/her deputies will be contacted for support. Where standard consents or notifications have been developed, employees are obligated to use those.
- In the event of a requirement to use Personal Information outside the consented purpose, then a further consent must be obtained from the Data Subject prior to such processing.
- The FSP will inform the Data Subject of the reasons for collecting his/her/its personal information, alternatively, where services or transactions are concluded over the telephone or electronically, the FSP will provide the stated purpose for collecting the personal information in an appropriate medium.
- The FSP will under no circumstances distribute or share personal information between separate legal entities, associated organisation's (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 and the reasons when their Personal Information will be shared with other associated organisations of the FSP.
- Where databases are provided by a third party, a warranty must be included in the contract that such database have been compiled in compliance with PoPIA and that the necessary consent was provided by the Data Subject.
- Only relevant Personal Information required for the specified purpose should be collected, nothing in excess of that. The data fields (see definition of "personal information" and "special information") in all existing and new databases and types of information (e.g. contracts, financial information, marketing lists, etc.) will be evaluated as to whether that specific data field is:
  - Necessary, given the specific purpose for which the personal information will be used.
  - Relevant for that purpose.

  Note: Red flag data fields are titles (relevant for communication, but not necessarily for the allocation of benefits), family relation (relevant for membership, but not for communication, etc.), information on race, gender, ethnicity (unless required by the B-BBEE Act, EEA, SDA or other law), physical address, views/opinions of persons, contact details (only what is relevant for that database should be kept), etc. The physical address of a trustee is necessary, but the address of a payments clerk at a customer or vendor is not required.
- Personal information is also collected from staff for employment purposes, such as payroll, tax, and deductions, leave administration, etc. Information on staff interviews and applications are kept until no longer needed.
- Personal information from the representatives, staff, agents, or contractors of vendors and suppliers are also processed for purposes of facilitating the financial services to be rendered.
- The information of persons responsible for accounts, finances, repair persons, key account managers and the likes are processed by the FSP for legitimate business purposes.

Condition 3: Purpose Specification

When Processing Personal Information as part of any activity, the FSP must:

- Identify the nature and extent to which one will deal with (a) Personal Information and (b) Special Personal Information (i.e. measure the data fields through which information it is collecting to assess whether it is relevant, necessary and not excessive), and then amend its processing accordingly.
- Identify the types of processing that will take place (e.g. collection, dissemination and destruction, or collection, recording and storage, etc.).
- Identify the purpose for which the specific processing is undertaken, clearly indicating whether such purpose is permitted by a law (e.g. invoicing requiring a VAT number).
- Confirm that consent has been obtained from Data Subjects, which consent shall constitute a contract between the FSP and the Data Subject and shall describe:
  - the purpose of the Processing or further processing of the Personal Information;
  - the type of Processing of the Personal Information;
  - timelines related to the Processing;
  - the destruction or storage of the personal information; and
  - the security assurances and measures undertaken by the FSP to protect the data and Personal Information.
- If processing is mandated by law, describe in a notification what that specific law says, and how processing will take place.

Personal Information about children and special personal information:

- The FSP may hold the personal information of children (persons up till the age of 18).
- The FSP may also have information of "child-dependents" older than 18, but who are still dependent on their parents – such persons are handled, for PoPIA purposes, the same as any adult dependent.
- The information of children under the age of 12, or between 12 and 18 years of age, must be processed in terms of the Children's Act, 2005.
- The FSP will take all reasonable measures to protect the confidentiality of adult dependents and children who have the right to confidentiality but acknowledges that there may be limitations to same when processing their information with product suppliers in the distribution chain.
- The FSP will only share information with third parties:
  - upon the specific consent of the Data Subject in terms of the Act and on written declaration that such third parties comply with the Act and related data legislation and regulations, or
  - if otherwise required to do so by any Applicable Law.

Condition 4: Further Processing Limitation

- Personal information will not be processed for a secondary purpose unless that processing is compatible with the original purpose.
- Where the FSP 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 FSP will first obtain additional consent from the Data Subject.

Condition 5: Information Quality

- The FSP will take reasonable steps to ensure that all personal information collected is complete, accurate, updated, and not misleading.

- Where personal information is collected or received from third parties, the FSP 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.

Condition 6: Open Communication

- The FSP must take reasonable steps to ensure that Data Subjects are notified and at all times aware, that their personal information is being collected, including the purpose for which it is being collected and processed.
- The FSP must ensure that it establishes and maintains a facility or communication method for Data Subjects who want to:
  - Enquire whether the FSP holds related personal information;
  - Request access to related personal information;
  - Request the FSP to update or correct related personal information; or
  - Make a complaint concerning the processing of personal information.

Condition 7: Security Safeguards and Measures

- The FSP 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.
- 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 FSP will continuously review its security controls, which will include regular testing of protocols and measures put in place to combat cyber-attacks on the FSP's IT network.
- The FSP 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 FSP 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 FSP's operators and third-party service providers will be required to enter into service level agreements with the FSP where both parties pledge their mutual commitment to PoPIA and the lawful processing of any personal information pursuant to the agreement.
- No FSP database, list, personal information of any person in its, or any staff member or office bearer's possession may be used, made known and/or distributed without the concerned Data Subjects' consent. In case of doubt, the advice of the Information Officer or his/her Deputy will be sought. Even casual provision of contact details to a third party could constitute a breach of the PoPIA.
- The FSP uses the following security measures to secure Personal Information in its possession:
  - Electronic information is secured by firewalls, anti-virus and password secured access;
  - Electronic information on shared drives operates on access control and permissions, accidental access must be reported to the Information Officer and IT immediately.

- No information, including personal information, may be downloaded from shared drives onto device hard drives or any external device.
- Physical records are kept at the office and protected by locking cabinets.
- The office has fingerprint access control at the respective doors.
- There are security cameras in the office.
- Office building is accessed through a boom gate.

- Regular verification that the safeguards in place are effectively implemented and continually updated in response to any new risks or deficiencies;
- Notification in writing to the affected Data Subjects and reporting to the Information Regulator, FSCA, and/or Insurer should the Personal Information relating to the Data Subject be compromised or should there be a suspicion that the Personal Information is compromised. All security and access breaches or suspected or potential breaches of personal information must be reported to the Information Regulator or his/her designated Deputy immediately after such breach or potential; breach becomes known.
- The Information Officer must ensure that the security measures are put in place for every database and type/category of personal information processed, to protect against:
  - **Unauthorised Access**, which means that access privileges must be stipulated, and where applicable, indicated in documents, minutes.
  - **Loss and/or damage of personal information**, through the following processes:
    - back-ups stored off-site and only accessible by certain staff;
    - remote wiping of computers and devices stolen/lost;
    - marking FSP owned property (such as devices, books, etc. that could contain personal information as "*confidential, property of the FSP, if found please return to [contact]),*
    - IT protections against file corruption, version control systems.
  - **Archiving and Destruction** will only take place in accordance with the FSP's Retention and Destruction Policy, and all archiving and destruction will be documented in the registers.

Condition 8: Data Subject Participation

- A Data Subject may request the correction or deletion of his/her/its personal information held by the FSP.
- The FSP must ensure that it provides a facility for Data Subjects who want to request the correction or deletion of their personal information.
- Where applicable, the FSP must include a link to unsubscribe from any of its electronic newsletters or related marketing activities.
- Only up to date and correct Personal Information can be processed, and Data Subjects can request the correction of their Personal Information on Form 2, see clause 23 below.
- All communications of a marketing or general communications nature must be subject to an "opt out" functionality, which has to be adhered to strictly by The FSP or anyone processing Personal Information for and on behalf of the FSP. The Data Subject's consent must be obtained on Form 4, see clause 23 below. Information related to changes to practice policies, any right, or legitimate expectation of a staff member, a supplier, or vendor cannot opt out of. Neither can they opt out of statements and similar information directly related to their contractual or other legal relationship with the FSP.

- All requests for Personal Information and other information from any person or entity whatsoever shall be dealt with in accordance with the provisions of the FSP's PAIA Manual and in line with this PoPIA Framework and Privacy Policy.
- All processing of Personal Information must immediately cease, in the event that the Data Subject withdraws its consent to the processing or objects to the processing of Personal Information in the manner prescribed by law, except where the FSP is by law obliged to continue with such processing. Such requests must be made to the FSP on Form 1 of the PoPIA Regulations, see clause 23 below.
- Personal Information must be corrected or deleted upon request by the Data Subject contained in Form 2, see clause 23 below.

9. Storage and Destruction

All Personal Information in the possession of the FSP must be stored, retained, and destroyed in accordance with the legislation applicable to the specific information and according to the FSP's Retention and Destruction provisions.

Personal Information shall not be retained longer than required to fulfil the purpose for the Processing or longer than required by Applicable Legislation.

Once the purpose for Processing or the retention period provided under Applicable Legislation expires, the Personal Information must be destructed, deleted, and/or returned to the Data Subject as may be required by the Applicable Law and in a manner that complies with such Applicable Law.

Retention periods, and the destruction of personal information, must be specified in consents and notifications.

10. Roles and Responsibilities

- **Information Officer**
  The FSP's Information Officer is responsible for:
  - Taking steps to ensure the FSP's reasonable compliance with the provision of PoPIA.
  - Keeping the governing body updated about the FSP's information protection responsibilities under PoPIA. For instance, in the case of a security breach, the Information Officer must inform and advise the governing body of their obligations pursuant to PoPIA.
  - Continually analysing privacy regulations and aligning them with the FSP's personal information processing procedures. This will include reviewing the FSP's information protection procedures and related policies.
  - Ensuring that PoPIA Audits are scheduled and conducted on a regular basis.
  - Ensuring that the FSP makes it convenient for Data Subjects who want to update their personal information or submit PoPIA related complaints to the FSP. For instance, maintaining a "contact us" facility on the FSP's website.
  - Approving any contracts entered into with Operators, employees, and other third parties which may have an impact on the personal information held by the FSP. This will include overseeing the amendment of the FSP's employment contract 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 FSP are fully aware of the risks associated with the processing of personal information and that they remain informed about the FSP's security controls.
- Organising and overseeing the awareness training of employees and other individuals involved in the processing of personal information on behalf of the FSP.
- Addressing employees PoPIA related questions.
- Addressing all PoPIA related requests and complaints made by the FSP's Data Subjects.
- Working with the Information Regulator in relation to any ongoing investigations. The Information Officer 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.
- Ensuring that a compliance framework is developed, implemented, monitored, and maintained.
- Ensuring that 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.
- Ensure that a manual is developed, monitored, maintained, and made available as prescribed in sections 14 and 51 of the Promotion of Access to Information Act.
- Ensure that internal measures are developed together with adequate systems to process requests for information or access thereto.
- Ensure that internal awareness sessions are conducted regarding the provisions of the Act, regulations made in terms of the Act, codes of conduct, or information obtained from the Regulator.
- The information officer shall upon request by any person, provide copies of the PAIA Manual to that person upon the payment of a fee to be determined by the Regulator from time to time.

- **IT Manager**

  The FSP's IT Manager is responsible for:

  - Ensuring that the FSP'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 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 FSP'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 operators or any other third-party service providers to process personal information on the FSP's behalf. For instance, cloud computing services.

- **Employees and Contractors**
  The FSP's Employees and other persons acting on behalf of the FSP must:
  - Treat personal information as a confidential business asset and to respect the privacy of Data Subjects.
  - Not directly or indirectly, utilise, disclose, or make public in any manner to any person or third party, either within the FSP 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.
  - 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.
  - Must ensure that s/he processes information in terms of the requirements, restrictions and limitations imposed by this PoPIA Framework and Privacy Policy.
  - Ensure that s/he fully understands and implements all of the FSP's policies and process relating to PoPIA.

11. Request to Access Personal Information Procedure

Whenever a request to Access Personal Information is made, the Data Subject must be provided with a copy of the FSP's PAIA and PoPIA Framework and Privacy Policy.

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 FSP's PAIA and PoPIA Framework and Privacy Policy.

12. Complaints Procedure

The FSP will address all PoPIA related complaints in accordance with the following procedure:

- PoPIA complaints must be submitted to the FSP in writing. Where so required, the Information Officer will provide the Data Subject with a "PoPIA Complaint Form – Annexure B" within 24 hours of being notified of the intention to lodge a complaint.
- The Information Officer will provide the complainant with a written acknowledgement of receipt of the complaint within 2 (two) working days.
- 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 FSP's Data Subject.
- Where the Information Officer has a 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 FSP's governing body, thereafter the affected Data Subjects, the Information Regulator, FSCA, and Insurer(s) will be informed of this breach.
- The Information Officer will revert to the complainant with an initial progress report within 10 days of receipt of the complaint. A further progress report will be supplied within 20 days of receipt of the complaint. The Information Officer will make a final decision with 30 days of receipt of the complaint. In all instances, the FSP will provide reasons for any decisions taken and communicate any anticipated deviations from the specified timelines.

- The Information Officers response to the Data Subject may comprise any of the following:
  - Uphold the complaint;
  - Rejection of the complaint;
  - 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 suggested remedies, the Data Subject has the right to complain to the Information Regulator.
- 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 needed. The reason for any complaints will also be reviewed to ensure the avoidance of occurrences giving rise to PoPIA related complaints.

13. Disciplinary Procedure

- The FSP will ensure that it follows its HR processes and procedures.
- The FSP 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 PoPIA Framework and Privacy Policy.
- The FSP may undertake to provide further awareness training to an employee in instances of minor negligence or misconduct.
- Any gross negligence or misconduct may result in the summary dismissal of the employee.
- The FSP may refer the employee to an appropriate law enforcement agency, Regulator and/or Authority for criminal investigation and/or may recover funds and assets in order to limit any prejudice or damages caused.

14. Information Officer

The FSP will appoint an Information Officer and where necessary, a Deputy Information Officer to assist the Information Officer.

The FSP's Information Officer is responsible for ensuring compliance with PoPIA. The Head of the FSP will assume the role of the Information Officer. Where the Head of the FSP has decided to authorise another employee of the FSP to be the Information Officer, such authorisation will be in writing according to the form and manner of "Annexure C".

The Information Officer must sign acceptance of his/her appointment as the Information Officer. This appointment letter will be used for the internal appointment of the Information Officer and/or Deputy Information Officer. The content of the appointment letter may also be incorporated into the designated employee's key performance areas as a measure to ensure accountability.

The Deputy Information Officer will assist the Information Officer in performing his/her duties. The Information Officer and/or Deputy Information Officer details for the FSP are as follows:

	INFORMATION OFFICER	DEPUTY INFORMATION OFFICER
Full Name	Tyrone Waterston	Byron Bosch
Designation	Managing Director	Legal and Compliance Manager
Contact Number	084 441 5357	079 382 4500
E-mail Address	tyrone@wwas.co.za	byron@wwas.co.za

All requests for information, complaints, contraventions, and non-compliance must be addressed to the Information Officer and/or the Deputy Information Officer on the applicable e-mail address provided above.

15. Training and Communication

All existing employees, contractors, vendors, committee members, and any person who may process Personal Information for and on behalf of the FSP, shall be trained on this PoPIA Framework and Privacy Policy and underlying legal sources on which it is based. The training will also form part of new employee induction. All Operators will be made aware of the FSP's PoPIA processes and procedures and will undertake to abide by same in terms of the Operator Agreement.

16. Compliance

The Information Officer shall maintain a report in relation to PoPIA and PAIA regarding steps and remedial steps taken in instances of non-compliance, including but not limited to:

- Re-wording of consents, standard clauses, and notifications.
- Reporting loss, breach and/or unauthorised access of Personal Information to relevant authorities, recommending disciplinary action, etc.
- The destruction of personal information.
- The de-identification of personal information.
- The implementation of specific security measures.
- The implementation of, additional or new, access control measures.
- The implementation of consents or notifications *ab initio*.
- Research and verification of legislative mandates.
- Addenda to contracts and service level agreements within business activities and/or with third parties and contractors.
- Amendments to contract templates.
- Disciplinary action against employees violating this PoPIA Framework and Privacy Policy.
- Action against office bearers violating this PoPIA Framework and Privacy Policy.
- Requirements on the submission of quarterly progress reports.
- Obtaining expert assistance, where required.
- Undergoing additional or further training on PoPIA and PAIA.

17. Complaints

Any complaints by any person including clients, members and beneficiaries, employees, third parties, or any Regulator, on any allegation or actual violation of this PoPIA Framework and Privacy Policy or data privacy, may be directed to the Information Officer, or a designated Deputy, who will handle the complaint and apply this PoPIA Framework and Privacy Policy, as well as the applicable laws and related policies of the FSP when doing so.

The Information Officer may constitute a Committee to investigate the matter, and to make findings on the complaint, and recommend action by the relevant departments. All Complaints must be lodged in writing, as per Annexure B.

18. PoPIA Act: Objections, Withdrawals, Amendments and Deletions

Any person can object to processing of Personal Information, withdraw a consent to processing, requests amend or deletion of personal Information. The forms to object, consent to marketing or request correction, deletion, or destruction of personal information are attached to this PoPIA Framework and Privacy Policy, as prescribed by the Regulations to the PoPIA published under GG number 42110 dated 14 December 2018, see clause 23 below.

19. Responsible Persons

DESCRIPTION	RESPONSIBLE PERSON
POPI Impact Assessment	Byron Bosch
Annual Review	Byron Bosch & Alida Govender (external Compliance Officer)
PoPIA Audits	Byron Bosch
PoPIA Training	Dedicated FSP training person
Liaison with Operators	Manager who is responsible for the specific business area
IT Manager	Paul Kruger

20. Review and Amendment

This PoPIA Framework and Privacy Policy shall be reviewed annually or more frequently as may be required and may be amended from time to time as may be required by law, for corrections of material errors or alignment with PoPIA risks identified, as the case may be.

21. Regulation Forms - As set out in the Regulations Published Under GG No. 42110 Dated 14 December 2018

The following documents or forms can be found on the Information Regulator's website: https://www.justice.gov.za alternatively, the Data Subject can request same from the FSP:

FORM 1	OBJECTION TO THE PROCESSING OF PERSONAL INFORMATION
FORM 2	REQUEST FOR CORRECTION OR DELETION OF PERSONAL INFORMATION OR DESTROYING OR DELETION OF RECORD OF PERSONAL INFORMATION
FORM 3	APPLICATION FOR THE ISSUE OF A CODE OF CONDUCT IN TERMS OF SECTION 61(1)*(B)*
FORM 4	APPLICATION FOR THE CONSENT OF A DATA SUBJECT FOR THE PROCESSING OF PERSONAL INFORMATION FOR THE PURPOSE OF DIRECT MARKETING
FORM 5	COMPLAINT REGARDING INTERFERENCE WITH THE PROTECTION OF PERSONAL INFORMATION/COMPLAINT REGARDING DETERMINATION OF AN ADJUDICATOR
FORM 6	NOTICE TO PARTIES: CONCILIATION MEETING REGARDING INTERFERENCE WITH THE PROTECTION OF PERSONAL INFORMATION
FORM 7	NOTICE TO PARTIES: CONCILIATION REGARDING INTERFERENCE WITH THE PROTECTION OF PERSONAL INFORMATION (CONCILIATION CERTIFICATE)
FORM 8	NOTICE TO PARTIES OF INTENTION OF REGULATOR TO INVESTIGATE A COMPLAINT
FORM 9	NOTICE TO PARTIES: SETTLEMENT MEETING REGARDING INTERFERENCE WITH THE PROTECTION OF PERSONAL INFORMATION
FORM 10	NOTICE TO PARTIES: SETTLEMENT REGARDING INTERFERENCE WITH THE PROTECTION OF PERSONAL INFORMATION
FORM 11	REQUEST FOR AN ASSESSMENT IN TERMS OF SECTION 89(1)
FORM 12	NOTIFICATION IN TERMS OF SECTION 89

FORM 13	NOTICE TO PARTIES NOT TO ISSUE AN ENFORCEMENT NOTICE IN TERMS OF SECTION 94
FORM 14	REFERRAL TO ENFORCEMENT COMMITTEE IN TERMS OF SECTION 92
FORM 15	ENFORCEMENT NOTICE IN TERMS OF SECTION 95
FORM 16	CANCELLATION OR VARIATION OF ENFORCEMENT NOTICE IN TERMS OF SECTION 96
FORM 17	NOTICE OF APPEAL IN TERMS OF SECTION 97
FORM 18	SUBSTITUTION OR SETTING ASIDE OF ENFORCEMENT NOTICE IN TERMS OF SECTION 98
FORM 19	NOTICE OF DISMISSAL OF APPEAL IN TERMS OF SECTION 98