PROTECTION OF PERSONAL INFORMATION POLICY

CONTROL MEASURES

- "ALOS" refers to ALOS Holdings (Pty) Ltd, ALOS Business Solutions (Pty) Ltd and ALOS Innovative Workforce Solutions (Pty) Ltd.
- We implemented control measures (actions, activities, processes and/or procedures) that will provide reasonable assurance that ALOS's compliance obligations are met and that non-compliances are prevented, detected, and corrected.
- Control measures are periodically evaluated and tested to ensure continuing effectiveness.

Action / Activity / Process / Procedure	Control Owner
Annual Review	Neil Harvey
Information Officer	Neil Harvey
Deputy Information Officer	Neil Harvey
POPI Audit	Neil Harvey
POPI Awareness Training	Neil Harvey

PROTECTION OF PERSONAL INFORMATION POLICY

Version	V1
Publishing Date	01/07/2021
Last Review Date	30/06/2021
Frequency of Review	Annually
Next Review Date	01/06/2022

POLICY STATEMENT:

- This policy forms part of the policy owner's internal business processes and procedures.
- ALOS's governing body, its employees, volunteers, contractors, suppliers and any other persons acting on behalf of ALOS are required to familiarise themselves with the policy's requirements and undertake to comply with the stated processes and procedures.
- Risk owners and control owners are responsible for overseeing and maintaining control procedures and activities.

POLICY ADOPTION:

Adoption of the processes and procedures outlined herein, was approved by:

Name & Surname	Ernest Sosias Coetzee
Capacity	Managing Director
Date	01/07/2021

TABLE OF CONTENTS

1. INTRODUCTION

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 through providing guiding principles that are intended to be applied to the processing of personal information in a context-sensitive manner.

Through the provision of quality goods and services, ALOS is necessarily involved in the collection, use and disclosure of certain aspects of the personal information of clients, customers, employees, and other stakeholders.

A person's right to privacy entails having control over his or her personal information and being able to conduct his or her affairs relatively free from unwanted intrusions.

Given the importance of privacy, ALOS is committed to effectively managing personal information in accordance with POPIA's provisions.

2. DEFINITIONS:

2.1 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.

2.2 Data Subject

This refers to the natural or juristic person to whom personal information relates, such as an individual client, customer or a company that supplies ALOS with products or other goods.

2.3 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.

2.4 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 ALOS 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.

2.5 Information Officer

The Information Officer is responsible for ensuring ALOS's compliance with POPIA.

Where no Information Officer is appointed, the head of ALOS 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 Officers can also be appointed to assist the Information Officer.

2.6 Processing

The act of processing information includes any activity or any set of operations, whether or not 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; or
- merging, linking, as well as any restriction, degradation, erasure or destruction of information.

2.7 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 so as to be capable, with or without the aid of some other equipment, of being reproduced.

2.8 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.

2.9 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.

2.10 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.

2.11 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.

2.12 Consent

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

2.13 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.

2.14 Biometrics

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

3. POLICY PURPOSE

This purpose of this policy is to protect ALOS from the compliance risks associated with the protection of personal information which includes:

- Breaches of confidentiality. For instance, ALOS could suffer loss in revenue where it is found that the personal information of data subjects has been shared or disclosed inappropriately.
- Failing to offer choice. For instance, all data subjects should be free to choose how and for what purpose ALOS uses information relating to them.
- Reputational damage. For instance, ALOS could suffer a decline in shareholder value following an adverse event such as a computer hacker deleting the personal information held by ALOS.

This policy demonstrates ALOS'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 ALOS.
- By assigning specific duties and responsibilities to control owners, including the appointment of an Information Officer and where necessary, Deputy Information Officers to protect the interests of ALOS 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.

4. POLICY APPLICATION

This policy and its guiding principles applies to:

- ALOS's governing body.
- All branches, business units and divisions of ALOS.
- All employees and volunteers.
- All contractors, customers, suppliers and other persons acting on behalf of ALOS.

The policy's guiding principles find application in all situations and must be read in conjunction with POPIA as well as ALOS'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.
- P**ersonal information**.
- Entered into a **record.**
- By or for a **responsible person**.
- Who is **domiciled** inside or outside of South-Africa.

POPIA does not apply in situations where the processing of personal information:

- is concluded in the course of purely personal or household activities, or
- where the personal information has been de-identified.

5. RIGHTS OF DATA SUBJECTS

Where appropriate, ALOS will ensure that its clients and customers are made aware of the rights conferred upon them as data subjects.

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

5.1 The Right to Access Personal Information

ALOS recognises that a data subject has the right to establish whether ALOS holds personal information related to him, her or it includes the right to request access to that personal information.

An example of a "Personal Information Request Form" can be found under Annexure A.

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 ALOS 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, ALOS will give due consideration to the request and the requirements of POPIA. ALOS 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.
An example of a "POPI Complaint Form" can be found under Annexure B.

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 ALOS.
The data subject also has the right to be notified in any situation where ALOS 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 employees and persons acting on behalf of ALOS 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 ALOS's reputation or expose ALOS to a civil claim for damages. The protection of personal information is therefore everybody's responsibility.

ALOS 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, ALOS 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

ALOS 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.

ALOS 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, ALOS will maintain a voice recording of the stated purpose for collecting the personal information followed by the data subject's subsequent consent.

ALOS 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 ALOS's business and be provided with the reasons for doing so.

6.3 Purpose Specification

All ALOS's business units and operations must be informed by the principle of transparency.

ALOS will process personal information only for specific, explicitly defined, and legitimate reasons. ALOS 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 ALOS 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, ALOS will first obtain additional consent from the data subject.

6.5 Information Quality

ALOS will take reasonable steps to ensure that all personal information collected is complete, accurate and not misleading.

The more important it is that the personal information be accurate, the greater the effort ALOS will put into ensuring its accuracy.

Where personal information is collected or received from third parties, ALOS 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

ALOS 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.

ALOS 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 ALOS holds related personal information, or
- Request access to related personal information, or
- Request ALOS to update or correct related personal information, or
- Make a complaint concerning the processing of personal information.

6.7 Security Safeguards

ALOS 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.

ALOS will continuously review its security controls which will include regular testing of protocols and measures put in place to combat cyber-attacks on ALOS's IT network.

ALOS 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 ALOS 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.

ALOS's operators and third-party service providers will be required to enter into service level agreements with ALOS 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 ALOS. ALOS will ensure that it provides a facility for data subjects who want to request the correction of deletion of their personal information.

Where applicable, ALOS will include a link to unsubscribe from any of its electronic newsletters or related marketing activities.

7. INFORMATION OFFICERS

ALOS appointed an Information Officer and where necessary, a Deputy Information Officer to assist the Information Officer.

ALOS's Information Officer is responsible for ensuring compliance with POPIA.

There are no legal requirements under POPIA for an organisation to appoint an Information Officer. Appointing an Information Officer is however, considered to be a good business practice, particularly within larger organisations.

Where no Information Officer is available, the head of ALOS will assume the role of the Information Officer.

Consideration will be given on an annual basis to the re-appointment or replacement of the Information Officer and the re-appointment or replacement of any Deputy Information Officers.

ALOS registered the Information Officer with the South African Information Regulator established under POPIA prior to performing his/her duties.

8. SPECIFIC DUTIES AND RESPONSIBILITIES

8.1 Governing Body

ALOS's governing body cannot delegate its accountability and is ultimately answerable for ensuring that ALOS 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:

- ALOS appointed an Information Officer, and a Deputy Information Officer.
- All persons responsible for the processing of personal information on behalf of ALOS:
  - 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 enquires 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 POPI Audit to accurately assess and review the ways in which ALOS collects, holds, uses, shares, discloses, destroys, and processes personal information.

8.2 Information Officer

ALOS's Information Officer is responsible for:

- Taking steps to ensure ALOS's reasonable compliance with the provision of POPIA.
- Keeping the governing body updated about ALOS'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 ALOS's personal information processing procedures. This will include reviewing ALOS's information protection procedures and related policies.
- Ensuring that POPI Audits are scheduled and conducted on a regular basis.
- Ensuring that ALOS makes it convenient for data subjects who want to update their personal information or submit POPI related complaints to ALOS. For instance, maintaining a "contact us" facility on ALOS's website.
- Approving any contracts entered with operators, employees and other third parties which may have an impact on the personal information held by ALOS. This will include overseeing the amendment of ALOS'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 ALOS are fully aware of the risks associated with the processing of personal information and that they remain informed about ALOS's security controls.
- Organising and overseeing the awareness training of employees and other individuals involved in the processing of personal information on behalf of ALOS.
- Addressing employees' POPIA related questions.
- Addressing all POPIA related requests and complaints made by ALOS'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, regarding any other matter.

  The Deputy Information Officer will assist the Information Officer in performing his or her duties.

8.3 IT Manager

ALOS's IT Manager is responsible for:

- Ensuring that ALOS'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 ALOS'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 ALOS's behalf. For instance, cloud computing services.

8.4 Marketing & Communication Manager

ALOS's Marketing & Communication Manager is responsible for:

- Approving and maintaining the protection of personal information statements and disclaimers that are displayed on ALOS'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 ALOS to ensure that any outsourced marketing initiatives comply with POPIA.

8.5 Employees and other Persons acting on behalf of ALOS

Employees and other persons acting on behalf of ALOS will, during the performance of their services, gain access to and become acquainted with the personal information of certain clients, suppliers, and other employees.

Employees and other persons acting on behalf of ALOS are required to treat personal information as a confidential business asset and to respect the privacy of data subjects.

Employees and other persons acting on behalf of ALOS may not directly or indirectly, utilise, disclose or make public in any manner to any person or third party, either within ALOS 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 and other persons acting on behalf of ALOS must 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.

Employees and other persons acting on behalf of ALOS 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 ALOS 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 ALOS with explicit written or verbally recorded consent to process his, her or its personal information.

Employees and other persons acting on behalf of ALOS 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, ALOS 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 and other persons acting on behalf of ALOS 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 ALOS's central database or a dedicated server.
- Share personal information informally. In particular, personal information should never be sent by email, as this form of communication is not secure. Where access to personal information is required, this may be requested from the relevant line manager or the Information Officer.
- Transfer personal information outside of South Africa without the express permission from the Information Officer.

Employees and other persons acting on behalf of ALOS are responsible for:

- Keeping all personal information that they encounter 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 ALOS, 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 such as external drives, CDs or DVDs that these are kept locked away securely when not being used.
- 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 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 to delete or dispose of the personal information in the appropriate manner.
- Undergoing POPI Awareness training from time to time.

  Where an employee, or a person acting on behalf of ALOS, 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 or the Deputy Information Officer.

9. POPI AUDIT

ALOS'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 ALOS. For instance, A L O S 's various business units, divisions, branches, and other associated organisations.
- Redefine the purpose for gathering and processing personal information.
- 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 extend of compliance with POPIA and this policy.
- Monitor the effectiveness of internal controls established to manage ALOS's POPI related compliance risk.

In performing the POPI Audit, Information Officers will liaise with line managers to identify areas within in ALOS'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 ALOS's governing body in performing their duties.

10. REQUEST TO ACCESS PERSONAL INFORMATION PROCEDURE

Data subjects have the right to:

- Request what personal information ALOS holds about them and why.
- Request access to their personal information.
- 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. The Information Officer will provide the data subject with a "Personal Information Request Form".

Once the completed form has been received, the Information Officer will verify the identity of the data subject prior to handing over any personal information. All requests will be processed and considered against ALOS's PAIA Policy.

The 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. ALOS takes all complaints very seriously and will address all POPI related complaints in accordance with the following procedure:

- POPI complaints must be submitted to ALOS in writing. Where so required, the Information Officer will provide the data subject with a "POPI Complaint Form".
- Where the complaint has been received by any person other than the Information Officer, that person will ensure that the full details of the complaint reach the Information Officer within 1 working day.
- The Information Officer will provide the complainant with a written acknowledgement of receipt of the complaint within 2 working days.
- The Information Officer will carefully consider the complaint and address the complainant's concerns in an amicable manner. In considering the complaint, the Information Officer will endeavour to resolve the complaint in a fair manner and in accordance with the principles outlined in POPIA.
- 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 ALOS's data subjects.
- Where the 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 ALOS's governing body where after the affected data subjects and the Information Regulator will be informed of this breach.
- The Information Officer will revert to the complainant with a proposed solution with the option of escalating the complaint to ALOS's governing body within 7 working days of receipt of the complaint. In all instances, ALOS will provide reasons for any decisions taken and communicate any anticipated deviation from the specified timelines.
- The Information Officer's 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 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 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, ALOS 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, ALOS will undertake to provide further awareness training to the employee.

Any gross negligence or the willful mismanagement of personal information, will be considered a serious form of misconduct for which ALOS 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 subsequent to 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.

ANNEXURE A: PERSONAL INFORMATION REQUEST FORM

PERSONAL INFORMATION REQUEST FORM

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

Please be aware that we may require you to provide proof of identification prior to processing your request.

There may also be a reasonable charge for providing copies of the information requested.

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

B. Request	
I request ALOS to:	
(a) Inform me whether it holds any of my personal information	☐
(b) Provide me with a record or description of my personal information	☐
(c) Correct or update my personal information	☐
(d) Destroy or delete a record of my personal information	☐

C. Instructions

D. Signature Page
Signature
Date

ANNEXURE B: POPI COMPLAINT FORM

POPI COMPLAINT FORM

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

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

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

The Information Regulator

Physical Address: JD House, 27 Stiemens Street, Braamfontein, Johannesburg, 2001

Email: inforeg@justice.gov.za / complaints.IR@justice.gov.za

Website: https://www.justice.gov.za/inforeg/contact.html

A. Particulars of Complainant	
Name & Surname	
Identity Number:	
Postal Address:	
Contact Number:	
Email Address:	
B. Details of Complaint	
C. Desired Outcome	
D. Signature Page	
Signature:	
Date	

ANNEXURE C: STATUTORY RETENTION PERIODS

Statutory Retention Periods		
Legislation	**Document Type**	**Period**
Companies Act	Any documents, accounts, books, writing, records or other information that a company is required to keep in terms of the Act; Notice and minutes of all Council Meetings, including resolutions adopted and documents made available to Council Members and Associations; Copies of reports presented at the annual general meeting of the company; Copies of annual financial statements required by the Act; Copies of accounting records as required by the Act; Record of directors and past directors, after the director has retired or resigned from the company; Written communication to Council Representatives; and Minutes and resolutions of Board Meetings or any other directors' meetings, and meetings of Board Committees, i.e. audit committee.	7 Years
	Registration certificate; Memorandum of Incorporation and alterations and amendments; Rules; Securities register and uncertified securities register; and Register of company secretary and auditors.	Indefinitely
Consumer Protection Act	Full names, physical address, postal address and contact details; ID number and registration number; Contact details of public officer in case of a juristic person; Service rendered; Cost to be recovered from the consumer; Frequency of accounting to the consumer; Amounts, sums, values, charges, fees, remuneration specified in monetary terms; and Conducting a promotional competition refer to Section 36(11)(b) and Regulation 11 of Promotional Competitions.	3 Years

Financial Intelligence Centre Act	Whenever a reportable transaction is concluded with a customer, the institution must keep record of the identity of the customer; If the customer is acting on behalf of another person, the identity of the person on whose behalf the customer is acting and the customer's authority to act on behalf of that other person; If another person is acting on behalf of the customer, the identity of that person and that other person's authority to act on behalf of the customer; The manner in which the identity of the persons referred to above was established; The nature of that business relationship or transaction; In the case of a transaction, the amount involved and the parties to that transaction; All accounts that are involved in the transactions concluded by that accountable institution in the course of that business relationship and that single transaction; The name of the person who obtained the identity of the person transacting on behalf of the accountable institution; and Any document or copy of a document obtained by the accountable institution.	5 Years
Compensation for Occupational Injuries and Diseases Act	Register, record or reproduction of the earnings, time worked, payment for piece work and overtime and other prescribed particulars of all the employees.	4 Years
	Section 20(2) documents: -Health and safety committee recommendations made to an employer in terms of issues affecting the health of employees and of any report made to an inspector in terms of the recommendation; and -Records of incidents reported at work.	3 Years
	Asbestos Regulations, 2001, regulation 16(1): -Records of assessment and air monitoring, and the asbestos inventory; -Medical surveillance records; Hazardous Biological Agents Regulations, 2001, Regulations 9(1) and (2): -Records of risk assessments and air monitoring; -Medical surveillance records. Lead Regulations, 2001, Regulation 10: -Records of assessments and air monitoring; -Medical surveillance records Noise - induced Hearing Loss Regulations, 2003, Regulation 11: -All records of assessment and noise monitoring; and -All medical surveillance records, including the baseline audiogram of every employee.	40 Years

	Hazardous Chemical Substance Regulations, 1995, Regulation 9: -Records of assessments and air monitoring; and -Medical surveillance records	30 Years
Basic Conditions of Employment Act	Section 29(4): -Written particulars of an employee after termination of employment; Section 31: -Employee's name and occupation; -Time worked by each employee; -Remuneration paid to each employee; and -Date of birth of any employee under the age of 18 years.	3 Years
Employment Equity Act	Records in respect of the company's workforce, employment equity plan and other records relevant to compliance with the Act; and Section 21 report which is sent to the Director General.	3 Years
Labour Relations Act	Records to be retained by the employer are the collective agreements and arbitration awards.	3 Years
	An employer must retain prescribed details of any strike, lock-out or protest action involving its employees; and Records of each employee specifying the nature of any disciplinary transgressions, the actions taken by the employer and the reasons for the actions.	Indefinitely
Unemployment Insurance Act	Employers must retain personal records of each of their current employees in terms of their names, identification number, monthly remuneration and address where the employee is employed.	5 Years
Tax Administration Act	Section 29 documents which: -Enable a person to observe the requirements of the Act; -Are specifically required under a Tax Act by the Commissioner by the public notice; and -Will enable SARS to be satisfied that the person has observed these requirements.	5 Years
Income Tax Act	Amount of remuneration paid or due by him to the employee; The amount of employee's tax deducted or withheld from the remuneration paid or due; The income tax reference number of that employee; Any further prescribed information; and Employer Reconciliation Return.	5 Years

Value Added Tax Act	Where a vendor's basis of accounting is changed the vendor shall prepare lists of debtors and creditors showing the amounts owing to the creditors at the end of the tax period immediately preceding the changeover period; Importation of goods, bill of entry, other documents prescribed by the Custom and Excise Act and proof that the VAT charge has been paid to SARS; Vendors are obliged to retain records of all goods and services, rate of tax applicable to the supply, list of suppliers or agents, invoices and tax invoices, credit and debit notes, bank statements, deposit slips, stock lists and paid cheques; Documentary proof substantiating the zero rating of supplies; and Where a tax invoice, credit or debit note, has been issued in relation to a supply by an agent or a bill of entry as described in the Customs and Excise Act, the agent shall maintain sufficient records to enable the name, address and VAT registration number of the principal to be ascertained.	5 Years