





Policy Title	PROTECTION OF PERSONAL INFORMATION ACT POLICY	ID Number	POPI 06/2021
Area of Impact	All	Effective Date	1 January 2021
Policy Owner	Jaco Beukes	Division	Corporate Services
Implemented by	Chantelle Nicole Fellingner Ariana Maraj	Developed by	Chantelle Nicole Fellingner Ariana Maraj

APPROVAL RECORD

	Name & Surname	Signature	Date
1st Review	Chantelle Nicole Fellingner	 Chantelle Fellingner (Jul 1, 2021 13:59 GMT+2)	Jul 1, 2021
2nd Review	HoD's	 Sunaina Singh (Jul 1, 2021 15:07 GMT+2)	Jul 1, 2021
Pre-approved by	Ariana Maraj	 Ariana Maraj (Jul 1, 2021 14:02 GMT+2)	Jul 1, 2021
Approved by	Jaco Beukes	 Jaco Beukes (Jul 1, 2021 18:45 GMT+2)	Jul 1, 2021

RECORD OF REVISIONS

Revision No	Date Approved	Nature of Revision	Prepared By



TERMS AND CONDITIONS OF USE

Use of all SAIL Rights Commercialisation (Pty) Limited, and its subsidiaries' policies and procedures on all its divisions constitutes your agreement to the following:

DOCUMENT OWNERSHIP

All content in this document is the property of SAIL Rights Commercialisation (Pty) Limited (“**SAIL**”) and all of its subsidiaries. All rights in this regard are strictly reserved. This document is for the use of SAIL, and its subsidiaries, employees only and authorised contractors or suppliers. The employee may not modify, copy, distribute, transmit, reproduce, publish, create derivative works from, transfer, or sell any information or services obtained from this document. In particular, use and distribution to competitor companies and/or previous employees and/or other third party who is not an employee of SAIL, and its subsidiaries, is strictly forbidden. Contravention by distributing to such parties constitutes an action that contravenes the company's rules and regulations which will result in disciplinary action and/or dismissal and/or claims for damages.

Client request for policies and procedures must be addressed through the HR/ Legal Division of SAIL where there is doubt as to what to distribute to a client. When in doubt, e-mail arian@sail.co.za.

Employee queries and clarification regarding policies to e-mail HR at ariana@sail.co.za

Agreement between employee and SAIL

Use of this document is conditional on acceptance by the employee of SAIL, and its subsidiaries' terms, conditions, and notices contained herein together with any additional policies or procedures on SAIL and its subsidiaries' Policy and Procedure Document Repository and elsewhere in the business from time to time by SAIL and/or its subsidiaries. By assessing and using this document, the employee is deemed to have agreed to all such terms, conditions and notices.

Contents

1.	INTRODUCTION	3
2.	DEFINITIONS	3
2.1	Personal Information	3
2.2	Data Subject	3
2.3	Responsible Party	4
2.4	Operator	4
2.5	Information Officer	4
2.6	Processing	4
2.7	Record	4
2.8	Filing System	5
2.9	Unique Identifier	5
2.10	De-Identify	5
2.11	Re-Identify	5
2.12	Consent	5
2.13	Direct Marketing	5
2.14	Biometrics	5
3.	POLICY PURPOSE	6
4.	POLICY APPLICATION	6
5.	RIGHTS OF DATA SUBJECTS	7
5.1	The Right to Access Personal Information	7
5.2	The Right to have Personal Information Corrected or Deleted	7
5.3	The Right to Object to the Processing of Personal Information	7
5.4	The Right to Object to Direct Marketing	7
5.5	The Right to Complain to the Information Regulator	7
5.6	The Right to be Informed	7
6.	GENERAL GUIDING PRINCIPLES	8
6.1	Accountability	8
6.2	Limitation	8
6.3	Purpose Specification	9
6.4	Further Processing Limitation	9
6.5	Information Quality	9
6.6	Open Communication	9
6.7	Security Safeguards	9
6.8	Data Subject Participation	10
8.	INFORMATION OFFICERS	11
9.	SPECIFIC DUTIES AND RESPONSIBILITIES	11
9.1	Information Officer	11
9.2	IT Manager	12
9.3	Corporate Services	13

9.4 Employees and other Persons acting on behalf of SAIL 13

10. POPI AUDIT 15

11. REQUEST TO ACCESS PERSONAL INFORMATION PROCEDURE 16

12. POPI COMPLAINTS PROCEDURE 16

13. DISCIPLINARY ACTION 17

ANNEXURE A: PERSONAL INFORMATION REQUEST FORM 19

ANNEXURE B: POPI COMPLAINT FORM..... 20

ANNEXURE C: POPI NOTICE AND CONSENT FORM 21

ANNEXURE D: EMPLOYEE CONSENT AND CONFIDENTIALITY CLAUSE..... 23

ANNEXURE E: SLA CONFIDENTIALITY CLAUSE 25

ANNEXURE F: STATUTORY RETENTION PERIODS.....28

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”). This policy and compliance framework establishes measures and standards for the protection and lawful processing of personal information within our organisation and provides principles regarding the rights of individuals to privacy and to reasonable safeguarding of their personal information. 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, SAIL 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, SAIL 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 SAIL 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. In this case, SAIL is the responsible party.

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 SAIL 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 SAIL's compliance with POPIA.

The Information Officer and Deputy Information Officer are set out below:

Abraham Jacobus Beukes – Information Officer

Chantelle Nicole Fellingner – Deputy Information Officer

The Information Officer and Deputy Information Officer have been registered with the South African Information Regulator established under POPIA.

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 make a donation of 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 and voice recognition.

3. POLICY PURPOSE

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

- Breaches of confidentiality. For instance, SAIL 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 SAIL uses information relating to them.
- Reputational damage. For instance, SAIL could suffer a decline in shareholder value following an adverse event such as a computer hacker deleting the personal information held by SAIL.

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

- All branches, business units and divisions of SAIL and its subsidiaries
- All employees, temporary employees, consultants and volunteer
- All contractors, suppliers and other persons acting on behalf of SAIL

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

The legal duty to comply with POPIA's provisions is activated in any situation where there is:

- A **processing of personal information** entered into a **record** by or for a **responsible person** who is **domiciled** in 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, SAIL will ensure that its clients and customers are made aware of the rights conferred upon them as data subjects.

SAIL will ensure that it gives effect to the following seven rights.

5.1 The Right to Access Personal Information

SAIL recognises that a data subject has the right to establish whether SAIL holds personal information related to him, her or it including 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 SAIL 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, SAIL will give due consideration to the request and the requirements of POPIA. SAIL 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 SAIL.

The data subject also has the right to be notified in any situation where SAIL 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

SAIL shall ensure that all processing conditions, as set out in POPIA, are complied with when determining the purpose and means of processing Personal Information and during the processing itself. All employees and persons acting on behalf of SAIL will at all times be subject to, and act in accordance with, the following guiding principles:

6.1 Accountability

Failing to comply with POPIA could potentially damage SAIL's reputation or expose SAIL to a civil claim for damages. The protection of personal information is therefore everybody's responsibility.

SAIL 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, SAIL 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. SAIL will take reasonable steps to ensure that personal, information obtained from employees will be stored safely and securely.

6.2 Limitation

SAIL 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.

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

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

An example of a "POPI Notice and Consent Form" can be found under **Annexure C**.

All Data Subjects have the right to refuse or withdraw their consent to the processing of their Personal Information, and a Data Subject may object, at any time, to the processing of their Personal Information on any of the above grounds, unless legislation provides for such processing. If the Data subject withdraws

consent or objects to processing then SAIL shall forthwith refrain from processing the Personal Information.

6.3 Purpose Specification

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

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

6.5 Information Quality

SAIL 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 (for example, the beneficiary details of a life insurance policy are of the utmost importance), the greater the effort SAIL will put into ensuring its accuracy.

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

SAIL will take reasonable steps to ensure that data subjects are notified (and are at all times aware) that their personal information is being collected including the purpose for which it is being collected and processed.

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

6.7 Security Safeguards

SAIL 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. The more sensitive the personal information, the greater the security required.

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

SAIL 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 SAIL 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.

SAIL's operators and third-party service providers will be required to enter into service level agreements with SAIL where both parties pledge their mutual commitment to POPIA and the lawful processing of any personal information pursuant to the agreement.

An example of "Employee Consent and Confidentiality Clause" for inclusion in SAIL's employment contracts can be found under **Annexure D**.

An example of an "SLA Confidentiality Clause" for inclusion in SAIL's agreements with clients and service providers can be found under **Annexure E**.

Any loss or theft of computers, laptops or other devices which may contain Personal Information must be immediately reported to the Information Officer, who shall notify the IT department, who shall take all necessary steps to remotely delete the information, if possible.

6.8 Data Subject Participation

A data subject may request the correction or deletion of his, her or its personal information held by SAIL.

SAIL will ensure that it provides a facility for data subjects who want to request the correction or deletion of their personal information.

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

7. DESTRUCTION OF DOCUMENTS

Documents may be destroyed after the termination of the retention period specified herein, or as determined by the Company from time to time. (Refer to annexure F - statutory retention periods)

Each department is responsible for attending to the destruction of its documents and electronic records, which must be done on a regular basis.

Files must be checked in order to make sure that they may be destroyed and also to ascertain if there are important original documents in the file. Original documents must be returned to the holder thereof, failing which, they should be retained by the Company pending such return.

The documents must be made available for collection by the Shred-It, or other approved document disposal company.

Deletion of electronic records must be done in consultation with the IT Department, to ensure that deleted information is incapable of being reconstructed and/or recovered.

8. INFORMATION OFFICERS

SAIL has appointed an Information Officer and a Deputy Information Officer to assist the Information Officer.

SAIL'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.

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.

SAIL has registered the Information Officer and Deputy Information Officer with the South African Information Regulator established under POPIA.

9. SPECIFIC DUTIES AND RESPONSIBILITIES

9.1 Information Officer

SAIL's Information Officer is responsible for:

- The development, implementation and monitoring of this policy and compliance framework.
- Ensuring this policy is supported by appropriate documentation.
- Ensuring that the documentation is relevant and kept up to date.
- Ensuring this policy and subsequent updates are communicated to relevant managers, representatives, staff and associates where applicable.
- Taking steps to ensure SAIL's reasonable compliance with the provision of POPIA.
- Keeping the governing body updated about SAIL's information protection responsibilities under POPIA. 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 SAIL's personal information processing procedures. This will include reviewing SAIL's information protection procedures and related policies.
- Ensuring that POPI Audits are scheduled and conducted on a regular basis.
- Ensuring that SAIL makes it convenient for data subjects who want to update their personal

information or submit POPI related complaints to SAIL. SAIL must maintain a “contact us” facility on its website.

- Approving any contracts entered into with operators, employees and other third parties which may have an impact on the personal information held by SAIL. This will include overseeing the amendment of SAIL’s employment contracts and agreements.
- Encouraging compliance with the conditions required for the lawful processing of personal information.
- Ensuring that employees and other persons acting on behalf of SAIL are fully aware of the risks associated with the processing of personal information and that they remain informed about SAIL’s security controls.
- Organising and overseeing the awareness training of employees and other individuals involved in the processing of personal information on behalf of SAIL.
- Addressing employees’ POPIA related questions.
- Addressing all POPIA related requests and complaints made by SAIL’s data subjects.
- Working with the Information Regulator in relation to any ongoing investigations. The Information Officers will therefore act as the contact point for the Information Regulator authority on issues relating to the processing of personal information and will consult with the Information Regulator where appropriate, with regard to any other matter.

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

9.2 IT Manager

SAIL’s IT Manager is responsible for:

- Ensuring that SAIL’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 shacking 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 SAIL’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 SAIL's behalf. For instance, cloud computing services.

9.3 Corporate Services

SAIL's head of Corporate Services, shall be responsible for:

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

9.4 Employees and other Persons acting on behalf of SAIL

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

Employees and other persons acting on behalf of SAIL 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 SAIL may not directly or indirectly, utilise, disclose or make public in any manner to any person or third party, either within SAIL 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 SAIL must request assistance from their head of division or the Deputy 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 SAIL 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 SAIL 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 SAIL with explicit written or verbally recorded consent to process his, her or its personal information.

Employees and other persons acting on behalf of SAIL 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, SAIL 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 SAIL 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 SAIL'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 head of division or the Deputy 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 SAIL are responsible for:

- Keeping all personal information that they come into contact with secure, by taking sensible precautions and following the guidelines outlined within this policy.
- Ensuring that personal information is held in as few places as is necessary. No unnecessary additional records, filing systems and data sets should therefore be created.

- Ensuring that personal information is encrypted prior to sending or sharing the information electronically. The IT Manager will assist employees and where required, other persons acting on behalf of SAIL, with the sending or sharing of personal information to or with authorised external persons and will ensure that such information is encrypted or password protected.
- 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 head of division or the Deputy Information Officer to update the information accordingly.
- Taking reasonable steps to ensure that personal information is stored only for as long as it is needed or required in terms of the purpose for which it was originally collected. Where personal information is no longer required, authorisation must first be obtained from the relevant head of division or the Deputy Information Officer to delete or dispose of the personal information in the appropriate manner.
- Undergoing POPI Awareness training from time to time.

Where an employee, or a person acting on behalf of SAIL, 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.

10. POPI AUDIT

SAIL's Information Officer will schedule annual 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 SAIL. For instance, SAIL's various business units, divisions, and where applicable, 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 SAIL's POPI related compliance risk.

In performing the POPI Audit, the Information and Deputy Information Officers will liaise with the head of divisions in order to identify areas within in SAIL's operation that are most vulnerable or susceptible to the unlawful processing of personal information.

Information and Deputy Information Officers will be permitted direct access to and have demonstrable support from its head of divisions in performing their duties.

11. REQUEST TO ACCESS PERSONAL INFORMATION PROCEDURE

Data subjects have the right to:

- Request what personal information SAIL 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 SAIL's PAIA Policy.

The Information Officer will process all requests within a reasonable time.

12. POPI COMPLAINTS PROCEDURE

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

- POPI complaints must be submitted to SAIL in writing. Where so required, the Information Officer or Deputy 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 SAIL'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 inform the affected data subjects and the Information Regulator of this breach.
- The Information Officer will revert to the complainant with a proposed solution with the option of escalating the complaint to the Information Regulator within 7 working days of receipt of the complaint. In all instances, SAIL 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.
- It is recorded that the Information Officer may delegate any and all of the responsibilities set out in this section to the Deputy information Officer.

13. DISCIPLINARY ACTION

Where a POPI complaint or a POPI infringement investigation has been finalised, SAIL 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, SAIL will undertake to provide further awareness training

to the employee.

Any gross negligence or the wilful mismanagement of personal information, will be considered a serious form of misconduct for which SAIL 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 in order to limit any prejudice or damages caused.


Jaco Beukes (Jul 1, 2021 18:45 GMT+2)

JACO BEUKES
CHIEF EXECUTIVE OFFICE

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 SAIL to:

(a) Inform me whether it holds any of my personal information	<input type="checkbox"/>
(b) Provide me with a record or description of my personal information	<input type="checkbox"/>
(c) Correct or update my personal information	<input type="checkbox"/>
(d) Destroy or delete a record of my personal information	<input type="checkbox"/>

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	Jaco Beukes Chantelle Fellingner
Contact Number	011 347 1300
Email Address:	jaco@sail.co.za chantellef@sail.co.za

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

The Information Regulator: Ms Mmamoroke Mphelo
Physical Address: SALU Building, 316 Thabo Sehume Street, Pretoria
Email: inforreg@justice.gov.za
Website: <http://www.justice.gov.za/inforeg/index.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: POPI NOTICE AND CONSENT FORM**POPI NOTICE AND CONSENT FORM**

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

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

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

Our Information Officer's Contact Details

Name	
Contact Number	
Email Address:	

Purpose for Processing your Information

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

- Providing you with advice, products and services that suit your needs as requested
- To verify your identity and to conduct credit reference searches, where applicable
- To process payments to or from you for advice, products and services purchased from us
- To notify you of new products or developments that may be of interest to you
- To confirm, verify and update your details
- To comply with any legal and regulatory requirements

Some of your information that we hold may include, your first and last name, email address, a home, postal or other physical address, other contact information, your title, birth date, gender, occupation, credit card details and your banking details.

Consent to Disclose and Share your Information

We may need to share your information to provide advice, reports, analyses, products or services that you have requested.

Where we share your information, we will take all precautions to ensure that the third party will treat your information with the same level of protection as required by us. Your information may be hosted on servers managed by a third-party service provider, which may be located outside of South Africa.

I hereby authorise and consent to SAIL sharing my personal information with the following persons:

Name & Surname
Signature
Date

ANNEXURE D: EMPLOYEE CONSENT AND CONFIDENTIALITY CLAUSE

EMPLOYEE CONSENT AND CONFIDENTIALITY CLAUSE

- “Personal Information” (PI) shall mean the 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 whether the information is recorded electronically or otherwise.
- “POPIA” shall mean the Protection of Personal Information Act 4 of 2013 as amended from time to time.
- The employer undertakes to process the PI of the employee only in accordance with the conditions of lawful processing as set out in terms of POPIA and in terms of the employer’s relevant policy available to the employee on request and only to the extent that it is necessary to discharge its obligations and to perform its functions as an employer and within the framework of the employment relationship and as required by South African law.
- The employee acknowledges that the collection of his/her PI is both necessary and requisite as a legal obligation, which falls within the scope of execution of the legal functions and obligations of the employer. The employee therefore irrevocably and unconditionally agrees:
 - That he/she is notified of the purpose and reason for the collection and processing of his or her PI insofar as it relates to the employer’s discharge of its obligations and to perform its functions as an employer.
 - That he/she consents and authorises the employer to undertake the collection, processing and further processing of the employee’s PI by the employer for the purposes of securing and further facilitating the employee’s employment with the employer.
 - Without derogating from the generality of the aforesaid, the employee consents to the employer’s collection and processing of PI pursuant to any of the employer’s Internet, Email and Interception policies in place insofar as PI of the employee is contained in relevant electronic communications.
 - To make available to the employer all necessary PI required by the employer for the purpose of securing and further facilitating the employee’s employment with the employer.
 - To absolve the employer from any liability in terms of POPIA for failing to obtain the employee’s consent or to notify the employee of the reason for the processing of any of the employee’s PI.
 - To the disclosure of his/her PI by the employer to any third party, where the employer has a legal or contractual duty to disclose such PI.
 - The employee further agrees to the disclosure of his/her PI for any reason enabling the employer to carry out or to comply with any business obligation the employer may have or to pursue a legitimate interest of the employer in order for the employer to perform its business on a day to day basis.
 - The employee authorises the employer to transfer his/her PI outside of the Republic of South Africa for any legitimate business purpose of the employer within the international community. The employer

undertakes not to transfer or disclose his/her PI unless it is required for its legitimate business requirements and shall comply strictly with legislative stipulations in this regard.

- The employee acknowledges that during the course of the performance of his/her services, he/she may gain access to and become acquainted with the personal information of certain clients, suppliers and other employees. The employee will treat personal information as a confidential business asset and agrees to respect the privacy of clients, suppliers and other employees.
- To the extent that he/she is exposed to or insofar as PI of other employees or third parties are disclosed to him/her, the employee hereby agree to be bound by appropriate and legally binding confidentiality and non-usage obligations in relation to the PI of third parties or employees.
- Employees may not directly or indirectly, utilise, disclose or make public in any manner to any person or third party, either within SAIL 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 on behalf of the employer.

ANNEXURE E: SLA CONFIDENTIALITY CLAUSE**SLA CONFIDENTIALITY CLAUSE**

- “Personal Information” (PI) shall mean the 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 whether the information is recorded electronically or otherwise.
- “POPIA” shall mean the Protection of Personal Information Act 4 of 2013 as amended from time to time.
- The parties acknowledge that for the purposes of this agreement that the parties may come into contact with, or have access to PI and other information that may be classified, or deemed as private or confidential and for which the other party is responsible. Such PI may also be deemed or considered as private and confidential as it relates to any third party who may be directly or indirectly associated with this agreement. Further, it is acknowledged and agreed by the parties that they have the necessary consent to share or disclose the PI and that the information may have value.
- The parties agree that they will at all times comply with POPIA’s Regulations and Codes of Conduct and that it shall only collect, use and process PI it comes into contact with pursuant to this agreement in a lawful manner, and only to the extent required to execute the services, or to provide the goods and to perform their respective obligations in terms of this agreement.
- The parties agree that it shall put in place, and at all times maintain, appropriate physical, technological and contractual security measures to ensure the protection and confidentiality of PI that it, or its employees, its contractors or other authorised individuals comes into contact with pursuant to this agreement.
- Unless so required by law, the parties agree that it shall not disclose any PI as defined in POPIA to any third party without the prior written consent of the other party, and notwithstanding anything to the contrary contained herein, shall any party in no manner whatsoever transfer any PI out of the Republic of South Africa.

ANNEXURE F: 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 shareholders meeting, including resolutions adopted and documents made available to holders of securities; 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 from the company; Written communication to holders of securities and Minutes and resolutions of directors' meetings, audit committee and directors' committees	7 years
	Registration certificate; Memorandum of Incorporation and alterations and amendments; Rules; Securities register and uncertified securities register; Register of company secretary and auditors and Regulated Companies (companies to which chapter 5, part B, C and Takeover Regulations apply) – Register of disclosure of person who holds beneficial interest equal to or in excess of 5% of the securities of that class issued.	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; 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; 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; -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; -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; -Medical surveillance records	30 years

<p>Basic Conditions of Employment Act</p>	<p>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; -Date of birth of any employee under the age of 18 years.</p>	<p>3 years</p>
<p>Employment equity Act</p>	<p>Records in respect of the company's workforce, employment equity plan and other records relevant to compliance with the Act; Section 21 report which is sent to the Director General</p>	<p>3 years</p>
<p>Labour Relations Act</p>	<p>Records to be retained by the employer are the collective agreements and arbitration awards.</p>	<p>3 years</p>
	<p>An employer must retain prescribed details of any strike, lock-out or protest action involving its employees; Records of each employee specifying the nature of any disciplinary transgressions, the actions taken by the employer and the reasons for the actions</p>	<p>Indefinite</p>
<p>Unemployment Insurance Act</p>	<p>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</p>	<p>5 years</p>
<p>Tax Administration Act</p>	<p>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; -Will enable SARS to be satisfied that the person has observed these requirements</p>	<p>5 years</p>

Income Tax Act	<p>Amount of remuneration paid or due by him to the employee;</p> <p>The amount of employees tax deducted or withheld from the remuneration paid or due;</p> <p>The income tax reference number of that employee;</p> <p>Any further prescribed information;</p> <p>Employer Reconciliation return.</p>	5 years
Value Added Tax Act	<p>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;</p> <p>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;</p> <p>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;</p> <p>Documentary proof substantiating the zero rating of supplies;</p> <p>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.</p>	5 years












POPI-policy-SAIL - Final - (300621)

Final Audit Report

2021-07-01

Created:	2021-07-01
By:	Chantelle Fellingner (chantellef@sail.co.za)
Status:	Signed
Transaction ID:	CBJCHBCAABAAiO97IYHZxWph1i8WCZUMfnhoHlbUa34

"POPI-policy-SAIL - Final - (300621)" History

-  Document created by Chantelle Fellingner (chantellef@sail.co.za)
2021-07-01 - 11:55:14 AM GMT- IP address: 197.234.197.170
-  Document e-signed by Chantelle Fellingner (chantellef@sail.co.za)
Signature Date: 2021-07-01 - 11:59:23 AM GMT - Time Source: server- IP address: 197.234.197.170
-  Document emailed to Ariana Maraj (ariana@sail.co.za) for signature
2021-07-01 - 11:59:25 AM GMT
-  Email viewed by Ariana Maraj (ariana@sail.co.za)
2021-07-01 - 12:01:35 PM GMT- IP address: 45.222.4.32
-  Document e-signed by Ariana Maraj (ariana@sail.co.za)
Signature Date: 2021-07-01 - 12:02:29 PM GMT - Time Source: server- IP address: 45.222.4.32
-  Document emailed to Sunaina Singh (sunaina@sail.co.za) for signature
2021-07-01 - 12:02:32 PM GMT
-  Email viewed by Sunaina Singh (sunaina@sail.co.za)
2021-07-01 - 12:23:13 PM GMT- IP address: 105.184.27.201
-  Document e-signed by Sunaina Singh (sunaina@sail.co.za)
Signature Date: 2021-07-01 - 1:07:39 PM GMT - Time Source: server- IP address: 105.184.27.201
-  Document emailed to Jaco Beukes (jaco@sail.co.za) for signature
2021-07-01 - 1:07:40 PM GMT
-  Email viewed by Jaco Beukes (jaco@sail.co.za)
2021-07-01 - 1:10:17 PM GMT- IP address: 169.0.211.231
-  Document e-signed by Jaco Beukes (jaco@sail.co.za)
Signature Date: 2021-07-01 - 4:45:20 PM GMT - Time Source: server- IP address: 169.0.211.231

✔ Agreement completed.

2021-07-01 - 4:45:20 PM GMT