

Set Sail Claims Consultants (Pty) Ltd
POPIA Policy
01 September 2025
Version 1

PROTECTION OF PERSONAL INFORMATION (POPIA) POLICY

SET SAIL CLAIMS CONSULTANTS (PTY) LTD

Registration Number: 2023/590963/07

*Prepared in accordance with the Protection of Personal Information Act 4 of 2013 and the
Regulations Relating to the Protection of Personal Information, 2018*

Set Sail Claims Consultants (Pty) Ltd
POPIA Policy
01 July 2025
Version 1

Document title	Set Sail Claims Consultants (Pty) Ltd POPIA Policy ("the Policy")
Document owner	Bruce Mark Lennon
Approved by	Director
Effective date	01 September 2025
Version	1.0
Next review date	01 September 2026 (annually)
Distribution	All Directors, Employees and Contractors of Set Sail Claims Consultants (Pty) Ltd.

This Policy supersedes any prior Data Privacy or POPIA Policy issued by Set Sail Claims Consultants (Pty) Ltd.

TABLE OF CONTENTS

1. Introduction and Purpose	5
1.1 Objectives.....	5
1.2 Status and binding effect	6
2. Scope and Application	7
3. Definitions	8
4. Information Officer and Deputy Information Officer.....	10
4.1 Designation	10
4.2 Registration with the Regulator	11
4.3 Duties	11
5. Conditions for Lawful Processing	12
5.1 Condition 1 — Accountability (section 8).....	12
5.2 Condition 2 — Processing Limitation (sections 9 to 12)	12
5.3 Condition 3 — Purpose Specification (sections 13 and 14).....	13
5.4 Condition 4 — Further Processing Limitation (section 15)	13
5.5 Condition 5 — Information Quality (section 16).....	13
5.6 Condition 6 — Openness (sections 17 and 18).....	13
5.7 Condition 7 — Security Safeguards (sections 19 to 22)	14
5.8 Condition 8 — Data Subject Participation (sections 23 to 25)	14
6. Categories of Data Subjects and Personal Information	15
7. Special Personal Information	17
8. Children's Personal Information	18
9. Lawful Basis for Processing	19
9.1 Consent.....	19
9.2 Contract.....	19
9.3 Legal obligation	20
9.4 Legitimate interests	20
10. Notification to Data Subjects (Section 18)	21
11. Sharing of Personal Information and Operators	22
11.1 Categories of recipients	22
11.2 Operator obligations (sections 20 and 21)	22
12. Trans-border Information Flows (Section 72)	23
13. Retention and Destruction of Records.....	24
13.1 General principle	24

13.2 Statutory retention periods	24
13.3 Destruction	25
14. Information Security Safeguards	26
14.1 Risk assessment	26
14.2 Technical safeguards.....	26
14.3 Organisational safeguards	27
14.4 Physical safeguards.....	27
14.5 Verification.....	27
15. Security Compromises (Breach Notification)	28
15.1 Internal escalation	28
15.2 Investigation	28
15.3 Notification to the Regulator.....	28
15.4 Notification to Data Subjects.....	29
15.5 Record of Security Compromises	29
16. Data Subject Rights	29
16.1 Right of access (section 23).....	30
16.2 Right to correction or deletion (section 24).....	30
16.3 Right to object (section 11(3)).....	30
16.4 Right to withdraw consent (section 11(2)(b)).....	31
16.5 Right not to be subject to automated decision-making (section 71).....	31
16.6 Right to lodge a complaint	31
17. Direct Marketing	31
17.1 Electronic direct marketing (section 69)	31
17.2 Other direct marketing	32
17.3 Suppression list	32
18. Automated Decision-Making	32
19. Complaints	33
19.1 Internal complaints	33
19.2 Complaints to the Regulator	33
20. Training, Awareness and Compliance Monitoring.....	34
21. Roles and Responsibilities	35
22. Policy Review.....	36
23. Information Regulator Contact Details.....	37

1. Introduction and Purpose

The Protection of Personal Information Act 4 of 2013 ("POPIA") gives effect to the constitutional right to privacy by regulating the manner in which Personal Information may be processed by Responsible Parties.¹

Set Sail Claims Consultants (Pty) Ltd ("the Company") is committed to protecting the privacy of all individuals and entities whose Personal Information it processes.

This Policy sets out how the Company collects, uses, stores, shares, secures and disposes of Personal Information in accordance with POPIA, the Regulations Relating to the Protection of Personal Information, 2018 ("the Regulations"), and any guidance issued by the Information Regulator.

1.1 Objectives

The objectives of this Policy are to:

- Articulate the eight Conditions for the lawful Processing of Personal Information set out in Chapter 3 of POPIA;
- Identify the rights of Data Subjects² and the procedures by which those rights may be exercised;
- Set out the obligations of the Information Officer, Deputy Information Officer, Employees, Directors and Contractors;
- Establish a defensible record of accountability for the Company's Processing activities; and
- Minimise the risk of unlawful Processing, Security Compromises and Regulatory Enforcement Action.

¹ POPIA came into full effect on 1 July 2020, and the one-year grace period for compliance ended on 30 June 2021.

² The person to whom Personal Information relates.

Set Sail Claims Consultants (Pty) Ltd
POPIA Policy
01 July 2025
Version 1

1.2 Status and binding effect

This Policy is binding on all Directors, Employees, Contractors and Agents³ of the Company. Breach of this Policy may result in disciplinary action up to and including dismissal, termination of contract, civil action and, where appropriate, referral to law enforcement authorities.

³ Contractors or Agents are persons/entities who Process Personal Information for a Responsible Party in terms of a contract or mandate, without coming under the direct authority of that Responsible Party.

2. Scope and Application

This Policy applies to all Personal Information processed by the Company, irrespective of format (electronic, paper, audio, visual or other), and to all Processing activities, whether automated or manual, performed by or on behalf of the Company.

This Policy applies to:

- All Personal Information of identifiable, living natural persons; and
- Where applicable, the Personal Information of identifiable, existing juristic persons.

This Policy does **not** apply to Processing of Personal Information that is excluded from POPIA in terms of section 6 of POPIA, including Processing in the course of a purely personal or household activity, de-identified information that cannot be re-identified, or Processing for journalistic, literary or artistic purposes to the extent that such Processing is subject to a code of ethics that provides adequate safeguards.

3. Definitions

Capitalised terms used in this Policy bear the meanings assigned to them in section 1 of POPIA.

The following key terms are highlighted for ease of reference:

Data Subject	The person to whom Personal Information relates.
Personal Information	Information relating to an identifiable, living natural person and, where applicable, an identifiable, existing juristic person — including (without limitation) name, identity number, contact details, biometric information, financial information, employment history, opinions and correspondence.
Special Personal Information	Personal Information concerning religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, biometric information, or criminal behaviour (alleged commission of an offence or any proceedings in respect of any offence).
Processing	Any operation or activity concerning Personal Information, including collection, receipt, recording, organisation, collation, storage, updating, retrieval, alteration, consultation, use, dissemination, merging, linking, restriction, degradation, erasure or destruction.
Responsible Party	A public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for Processing Personal Information. The Company is the Responsible Party for purposes of this Policy.
Contractor or Agent	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 Responsible Party.
Information Officer	The Head of the Company, or a person duly designated by the Head, who bears the duties set out in section 55 of POPIA and Regulation 4 of the Regulations.

Set Sail Claims Consultants (Pty) Ltd
POPIA Policy
01 July 2025
Version 1

Deputy Information Officer	Any person designated under section 56 of POPIA, read with section 17 of PAIA, to assist the Information Officer.
Regulator	The Information Regulator established in terms of section 39 of POPIA.
Consent	Any voluntary, specific and informed expression of will by which a Data Subject agrees to the Processing of Personal Information.
Security Compromise	Any incident in which there are reasonable grounds to believe that Personal Information has been accessed or acquired by an unauthorised person, as contemplated in section 22 of POPIA.
PAIA	Promotion of Access to Information Act 2 of 2000 (as amended)

4. Information Officer and Deputy Information Officer

4.1 Designation

In terms of section 56 of POPIA, the Head of the Company is the Information Officer by operation of law. The Head may designate one or more Deputy Information Officers to perform the duties set out in section 55 of POPIA.

The Company has designated the following individuals:

Information Officer	Bruce Mark Lennon
Position	Director
Email	bruce@setsailclaims.com
Telephone	+27 (0)31 396 7501
Mobile	+27 (0)83 788 7778
Deputy Information Officer	Damon Stephenson
Position	Head of Claims
Email	damon@setsailclaims.com
Telephone	+27 (0)31 396 7501
Mobile	+27 (0)76 317 6030
Postal address	Suite 5, 1 st Floor, Aloe Block, Fairway Green Office Park, 3 Abrey Road, Kloof, 3610, South Africa
Physical address	Suite 5, 1 st Floor, Aloe Block, Fairway Green Office Park, 3 Abrey Road, Kloof, 3610, South Africa

4.2 Registration with the Regulator

The Information Officer (and any Deputy Information Officer) must be registered with the Information Regulator via the Regulator's eServices Portal⁴ before taking up their duties. Registration is the personal responsibility of the Information Officer and must be kept current.

4.3 Duties

The Information Officer is responsible for:

- Encouraging compliance by the Company with the Conditions for the lawful Processing of Personal Information;
- Dealing with requests made to the Company pursuant to POPIA and PAIA;
- Working with the Information Regulator in relation to investigations conducted under POPIA;
- Ensuring that a compliance framework is developed, implemented, monitored and maintained;
- Ensuring that a personal information impact assessment is conducted to ensure that adequate measures and standards exist to comply with the Conditions for lawful Processing;
- Ensuring that a Personal Information Protection (POPIA) policy is developed, implemented, monitored and maintained;
- Ensuring that internal awareness sessions are conducted regarding the provisions of POPIA, the Regulations, Codes of Conduct and this Policy;
- Ensuring that the Company maintains a section 17 record of all Processing operations under its responsibility; and
- Ensuring that copies of the PAIA Manual are made available as prescribed by law.

⁴ <https://eservices.inforegulator.org.za>

5. Conditions for Lawful Processing

Chapter 3 of POPIA prescribes 8 (eight) Conditions for the lawful Processing of Personal Information. The Company commits to giving effect to each Condition in all of its Processing activities.

5.1 Condition 1 — Accountability (section 8 of POPIA)

The Company, as Responsible Party, ensures that the Conditions set out in Chapter 3 of POPIA, and all the measures that give effect to those Conditions, are complied with at the time of the determination of the purpose and means of Processing, and during the Processing itself.

5.2 Condition 2 — Processing Limitation (sections 9 to 12 of POPIA)

Personal Information is processed lawfully and in a reasonable manner by the Company, so as to ensure that it does not infringe the privacy of the Data Subject. Processing is limited to information that is adequate, relevant and not excessive having regard to the purpose for which it is processed.

Processing takes place only where one of the lawful bases in section 11(1) of POPIA is established, namely:

- The Data Subject (or a competent person where the Data Subject is a child) has consented;
- Processing is necessary to carry out actions for the conclusion or performance of a contract to which the Data Subject is party;
- Processing complies with an obligation imposed by law on the Responsible Party;
- Processing protects a legitimate interest of the Data Subject;
- Processing is necessary for the proper performance of a public law duty by a public body; or
- Processing is necessary for pursuing the legitimate interests of the Responsible Party or of a Third Party to whom the information is supplied.

Personal Information is collected directly from the Data Subject, unless one of the exceptions in section 12(2) of POPIA applies (for example, where the information is contained in a public record or has been deliberately made public by the Data Subject, or where collection from another source would not prejudice a legitimate interest).

5.3 Condition 3 — Purpose Specification (sections 13 and 14 of POPIA)

Personal Information is collected for a specific, explicitly defined and lawful purpose related to a function or activity of the Company. Records of Personal Information are not retained any longer than is necessary for achieving the purpose for which they were collected, unless retention is required or authorised by law, or the Data Subject (or a competent person where the Data Subject is a child) has consented to longer retention.

5.4 Condition 4 — Further Processing Limitation (section 15)

Further Processing of Personal Information is only undertaken where it is in accordance with, or compatible with, the purpose for which it was originally collected. Where the further Processing would not be compatible, the Company will obtain fresh consent or rely on another lawful basis as set out in section 15(3) of POPIA.

5.5 Condition 5 — Information Quality (section 16 of POPIA)

The Company takes reasonably practicable steps to ensure that the Personal Information it processes is complete, accurate, not misleading and updated where necessary. In doing so, the Company has regard to the purpose for which the Personal Information is collected or further processed.

5.6 Condition 6 — Openness (sections 17 and 18 of POPIA)

The Company maintains documentation of all Processing operations under its responsibility, as required by section 17 of POPIA, in its section 17 record of Processing activities, and in its PAIA Manual.

Set Sail Claims Consultants (Pty) Ltd
POPIA Policy
01 July 2025
Version 1

When collecting Personal Information, the Company takes reasonably practicable steps to ensure that the Data Subject is aware of the matters specified in section 18(1) of POPIA, as set out in clause 10 of this Policy.

5.7 Condition 7 — Security Safeguards (sections 19 to 22 of POPIA)

The Company secures the integrity and confidentiality of Personal Information in its possession or under its control by taking appropriate, reasonable technical and organisational measures, as set out in clauses 14 and 15 of this Policy – as set out below.

5.8 Condition 8 — Data Subject Participation (sections 23 to 25 of POPIA)

The Company gives effect to the rights of Data Subjects to access, correct, delete or destroy Personal Information held about them, as set out in clause 16 of this Policy.

6. Categories of Data Subjects and Personal Information

The Company processes Personal Information in respect of the following categories of Data Subjects. The list is indicative and is not exhaustive.

A detailed register is maintained in the Company's section 17 record of Processing activities.

Category of Data Subject	Categories of Personal Information	Purpose of Processing
Client / Clients (natural persons)	Names, identity number, contact details, physical and postal address, banking and payment details, correspondence, claims history.	Provision of services; performance of contracts; invoicing; Client support; legal compliance.
Client / Clients (juristic persons)	Registered name, registration number, contact persons and their contact details, banking details, tax information, beneficial ownership and claims history.	Provision of services; performance of contracts; invoicing; Client support; KYC and FICA; legal compliance.
Suppliers and service providers	Contact persons, contact details, banking details, registration documents, tax clearance, BBBEE certificates.	Procurement; payment; supplier due diligence; legal and regulatory compliance.
Employees and job applicants	Names, ID number, contact details, qualifications, employment history, banking, tax and medical aid details, performance information.	HR administration; payroll; statutory reporting; performance management; recruitment.
Directors, shareholders and officers	Names, ID number, contact details, banking details, share / directorship records.	Statutory and corporate governance compliance.

Set Sail Claims Consultants (Pty) Ltd
POPIA Policy
01 July 2025
Version 1

Category of Data Subject	Categories of Personal Information	Purpose of Processing
Website visitors and electronic users	IP address, device information, usage data, contact details submitted via forms.	Website operation; analytics; marketing.

7. Special Personal Information

Section 26 of POPIA prohibits the Processing of Special Personal Information unless one of the general authorisations in section 27 of POPIA, or one of the specific authorisations in sections 28 to 33 of POPIA, applies.

Where the Company processes Special Personal Information, the responsible business unit must, in consultation with the Information Officer, identify and document the lawful authorisation relied upon and the safeguards applied.

Special Personal Information processed by the Company may include:

- Health information of Employees (for occupational health, medical aid and disability administration);
- Biometric information (where used for access control or time and attendance, subject to a documented purpose and Data Subject notification);
- Information on alleged criminal conduct (for purposes of pre-employment screening, disciplinary processes, fraud investigations or litigation); and
- Race or ethnic origin (where required for compliance with employment equity, B-BBEE and/or affirmative action obligations).

Special Personal Information must be subject to enhanced security safeguards including, where reasonably practicable, encryption, restricted access on a need-to-know basis, and segregated storage.

8. Children's Personal Information

Section 34 of POPIA prohibits the Processing of Personal Information of a child unless one of the general authorisations in section 35 of POPIA applies — including:

- (a) Processing carried out with the prior consent of a competent person; and/or
- (b) Processing necessary for the establishment, exercise or defence of a right or obligation in law; and/or
- (c) Processing necessary to comply with an obligation of international public law; and/or
- (d) Processing for historical, statistical or research purposes subject to specified Safeguards; and/or
- (e) Processing of information deliberately made public by the child with the consent of a competent person.

A "child" means a natural person under 18 years of age who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him- or herself.

The Company will not knowingly process the Personal Information of a child without the prior, demonstrable consent of a competent person, or another lawful authorisation under section 35 of POPIA.

Any business unit of the Company that proposes to process the Personal Information of children must consult the Information Officer in advance and ensure that an appropriate consent and verification mechanism is in place.

9. Lawful Basis for Processing

Each Processing activity undertaken by the Company must be supported by at least one lawful basis under section 11(1) of POPIA. The Company maintains a register of Processing activities, mapped to lawful bases, in its section 17 record.

The register is reviewed at least annually by the Information Officer.

9.1 Consent

Where Processing is based on consent, the consent must be voluntary, specific and informed.

Consent must be obtained at or before the point of collection and must be capable of being demonstrated by the Company.

A Data Subject may withdraw consent at any time, provided that the lawfulness of Processing prior to the withdrawal remains unaffected.

9.2 Contract

Where Processing is necessary for the conclusion or performance of a contract to which the Data Subject is a Party, no separate consent is required.

The Company will, however, ensure that the Data Subject is informed of the Processing in terms of section 18 of POPIA.

9.3 Legal obligation

Where Processing is required to comply with an obligation imposed by law (for example, the Companies Act⁵, the Tax Administration Act⁶, the Basic Conditions of Employment Act⁷, the Labour Relations Act⁸, the Financial Intelligence Centre Act⁹ or the Compensation for Occupational Injuries and Diseases Act¹⁰), the relevant statutory provision must be identified and recorded in the section 17 record.

9.4 Legitimate interests

Where Processing is based on the legitimate interests of the Company, of the Data Subject or of a Third Party, the Information Officer must approve a written legitimate interests' assessment that records the interest pursued, the necessity of the Processing, and the balancing of interests against the rights and reasonable expectations of the Data Subject.

⁵ 71 of 2008 (as amended)

⁶ 28 of 2011 (as amended)

⁷ 75 of 1997 (as amended)

⁸ 66 of 1995 (as amended)

⁹ 38 of 2001 (as amended)

¹⁰ 130 of 1993 (as amended)

10. Notification to Data Subjects (Section 18 of POPIA)

When Personal Information is collected, the Company will take reasonably practicable steps to ensure that the Data Subject is aware of the following:

- The information being collected and, where the information is not collected from the Data Subject, the source from which it is collected;
- The name and address of the Responsible Party;
- The purpose for which the information is being collected;
- Whether or not the supply of the information is voluntary or mandatory;
- The consequences of failure to provide the information;
- Any particular law authorising or requiring the collection of the information;
- Whether the Company intends to transfer the information to a third country or international organisation, and the level of protection afforded to the information by that country or organisation; and
- Any further information such as the recipient or category of recipients of the information; the nature or category of the information; the existence of the right of access to and the right to rectify the information collected; the existence of the right to object to the Processing; and the right to lodge a complaint with the Information Regulator.

Notification is given by means of a Privacy Notice published on the Company's website and, where appropriate, by means of bespoke notices included in Employment Contracts, Client Onboarding Documents and Supplier Agreements.

11. Sharing of Personal Information and Contractors/Agents

11.1 Categories of recipients

The Company may share Personal Information with the following categories of recipients:

- Contractors engaged by the Company (including, without limitation, IT and cloud service providers, payroll bureaus, medical aid administrators, Employee assistance programme providers, debt collectors, courier and postal services, and external auditors);
- Professional advisors of the Company, including attorneys, accountants and consultants, subject to a duty of confidentiality;
- Regulators, supervisory bodies and other public bodies, where required by law; and
- Courts, tribunals, arbitrators and law enforcement authorities, where required by law or court order.

11.2 Contractor obligations (sections 20 and 21 of POPIA)

Where the Company appoints a Contractor, the Contractor is legally obligated to in terms of contract to Process Personal Information only with the knowledge or authorisation of the Company, and treat Personal Information that comes to its knowledge as confidential.

The appointment must be governed by a written contract that requires the Contractor to:

- Establish and maintain appropriate, reasonable technical and organisational measures to secure the integrity and confidentiality of Personal Information, in compliance with section 19 of POPIA;
- Notify the Company immediately, and in any event without undue delay, of any Security Compromise;
- Process Personal Information only on documented instructions from the Company;
- Ensure that persons authorised to Process Personal Information are subject to a duty of confidentiality;
- Not engage a sub-contractor without the prior written authorisation of the Company; and

- On termination of the engagement, return or destroy all Personal Information processed on behalf of the Company.

The Information Officer maintains a register of Contractors.

No new Contractor may be engaged without due diligence and the conclusion of a written contract that satisfies sections 20 and 21 of POPIA.

12. Trans-border Information Flows (Section 72 of POPIA)

The Company may transfer Personal Information about a Data Subject to a Third Party in a foreign country only where one or more of the following grounds in section 72 of POPIA applies:

- The Third Party is subject to a law, binding corporate rules or binding agreement that provides an adequate level of protection that effectively upholds principles for reasonable Processing substantially similar to the conditions in POPIA, and that includes provisions substantially similar to section 72 of POPIA in respect of onward transfers; and/or
- The Data Subject has consented to the transfer; and/or
- The transfer is necessary for the performance of a contract between the Data Subject and the Responsible Party, or for the implementation of pre-contractual measures taken in response to the Data Subject's request; and/or
- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the Responsible Party and a Third Party; and/or
- The transfer is for the benefit of the Data Subject and it is not reasonably practicable to obtain consent, and if it were, the Data Subject would be likely to give it.

Before any new trans-border transfer is affected, the responsible business unit of the Company must consult the Information Officer, who will record the lawful ground relied upon and confirm that the appropriate safeguards are in place.

Standard cloud and software-as-a-service arrangements are addressed by the Contractor agreement requirements in clause 11.2 above, including, where appropriate, the use of Standard Contractual Clauses or equivalent data-transfer mechanisms.

13. Retention and Destruction of Records

13.1 General principle

In accordance with section 14 of POPIA, records of Personal Information are not retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed, unless:

- Retention of the record is required or authorised by law; and/or
- The Company reasonably requires the record for lawful purposes related to its functions or activities; and/or
- Retention of the record is required by a contract between the parties; and/or
- The Data Subject (or a competent person where the Data Subject is a child) has consented to the retention of the record.

13.2 Statutory retention periods

Without limiting the general principle above, the Company applies the following statutory retention periods.

Where 2 (two) or more periods apply to the same record, the longer applies:

Companies Act 71 of 2008	7 (seven) years (or longer if statutorily required) for accounting records, financial statements, securities register, register of directors and notices to shareholders.
Tax Administration Act 28 of 2011 / Income Tax Act 58 of 1962 / VAT Act 89 of 1991	5 (five) years from the date of submission of the return, or longer where an audit, objection or appeal is pending.

Basic Conditions of Employment Act 75 of 1997	3 (three) years after termination of employment for time and remuneration records.
Labour Relations Act 66 of 1995	3 (three) years for records of strike, lock-out and protest action.
Employment Equity Act 55 of 1998	Period prescribed in the Act for employment equity records.
Skills Development Act 97 of 1998 / Levies Act	5 (five) years for skills development records and returns.
Compensation for Occupational Injuries and Diseases Act 130 of 1993	4 (four) years for register of injuries and accidents.
Occupational Health and Safety Act 85 of 1993	3 (three) years for general administration and training records 5 (five) years for accident/incident reports 20 (twenty) years for injuries on duty 5 (five) years for general sick leave and medical certificates/notes 10 (ten) years for fitness-for-work assessments/medicals
Financial Intelligence Centre Act 38 of 2001 (where applicable)	5 (five) years from the end of the business relationship or completion of the transaction.
Consumer Protection Act 68 of 2008	3 (three) years for records of consumer transactions where applicable.

13.3 Destruction

On expiry of the applicable retention period, records of Personal Information must be destroyed, deleted or de-identified in a manner that prevents reconstruction in an intelligible form:

- Paper records must be securely shredded; and

- Electronic records must be deleted using methods that render the information irrecoverable.

The destruction of records must be logged.

14. Information Security Safeguards

In accordance with section 19 of POPIA, the Company secures the integrity and confidentiality of Personal Information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent loss of, damage to, or unauthorised destruction of Personal Information, and unlawful access to or Processing of Personal Information.

14.1 Risk assessment

The Company has identified all reasonably foreseeable internal and external risks to Personal Information in its possession or under its control, and has established and maintains appropriate safeguards against the risks identified.

The risk assessment is reviewed at least annually.

14.2 Technical safeguards

The Company has implemented the following appropriate and reasonable technical safeguards in protecting the Personal Information of Data Subjects in its possession:

- Network firewalls, intrusion detection and intrusion prevention systems;
- Anti-malware and end-point protection software with current signature updates;
- Logging of access to and changes in systems containing Personal Information; and
- Secure backup and Disaster Recovery Plan.

14.3 Organisational safeguards

The Company has implemented the following appropriate and reasonable organisational safeguards in protecting the Personal Information of Data Subjects in its possession:

- Written policies governing acceptable use, access management, mobile devices, remote work and clean-desk practices;
- Written confidentiality undertakings from all Employees, contractors and Operators;
- Regular awareness training for Employees on POPIA, information security and phishing;
- Background checks for Employees in positions of trust; and
- A documented Incident Response Plan.

14.4 Physical safeguards

The Company has implemented the following appropriate and reasonable physical safeguards in protecting the Personal Information of Data Subjects in its possession:

- Controlled access to premises;
- Secure storage (locked cabinets, safes or restricted-access rooms) for paper records and removable media; and
- Secure disposal of confidential waste.

14.5 Verification

The Information Officer is responsible for ensuring that the safeguards are continually updated in response to new risks or deficiencies.

The Company verifies the effectiveness of safeguards through annual reviews, audits and testing.

15. Security Compromises (Breach Notification)

Where there are reasonable grounds to believe that Personal Information of a Data Subject has been accessed or acquired by an unauthorised person, section 22 of POPIA requires the Company to notify the Information Regulator and the affected Data Subject as soon as reasonably possible.

15.1 Internal escalation

Any Employee or Contractor who becomes aware of an actual or suspected Security Compromise must report it immediately (within 24 hours of becoming aware) to the Information Officer using the Internal Security Incident Report (Annexure *** hereto).

15.2 Investigation

The Information Officer will, with the assistance of the Deputy Information Officer:

- Investigate the incident;
- Contain the compromise;
- Identify the categories of Personal Information and Data Subjects affected; and
- Assess the risk to Data Subjects.

15.3 Notification to the Regulator

Where notification is required, the Company will notify the Information Regulator using the prescribed notification mechanism.

The notification will set out:

- A description of the nature and extent of the Security Compromise;
- A description of the possible consequences of the Security Compromise;
- A description of the measures the Company intends to take or has taken to address the Security Compromise;

- A recommendation with regard to the measures to be taken by the Data Subject to mitigate the possible adverse effects of the Security Compromise; and
- If known to the Company, the identity of the unauthorised person who may have accessed or acquired the Personal Information.

15.4 Notification to Data Subjects

The notification to the affected Data Subject(s) must be communicated in writing in at least 1 (one) of the prescribed ways:

- Mail to the last known physical or postal address;
- Email to the last known email address;
- Placement in a prominent position on the Company website;
- Publication in the news media; and/or
- As may be directed by the Regulator.

Notification to the Data Subject(s) may only be delayed if a public body responsible for the prevention, detection or investigation of offences, or the Regulator, determines that notification will impede a criminal investigation.

15.5 Record of Security Compromises

The Information Officer maintains a register of all Security Compromises, including those that did not require notification, with sufficient detail to allow the Regulator to verify compliance with section 22 of POPIA.

16. Data Subject Rights

Data Subjects have the rights set out in section 5 of POPIA.

The Company gives effect to those rights as follows:

- All requests must be directed to the Information Officer at the contact details in clause 4; and

- The Company will respond as soon as reasonably possible, and in any event within 30 (thirty) days of receipt, unless an extension is lawfully required.

16.1 Right of access (section 23 of POPIA)

A Data Subject may request confirmation of whether the Company holds Personal Information about him/her/it, and may request the record or a description of the Personal Information held, including information about the identity of all third parties who have, or have had, access to the information.

Requests for access are processed in terms of PAIA¹¹

16.2 Right to correction or deletion (section 24 of POPIA)

A Data Subject may request the Company to correct or delete Personal Information that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully, or to destroy or delete a record of Personal Information that the Company is no longer authorised to retain.

Requests must be made on POPIA Form 2.¹²

16.3 Right to object (section 11(3) of POPIA)

A Data Subject may object, on reasonable grounds relating to his/her/its particular situation, to the Processing of Personal Information based on legitimate interests or public interest.

The Data Subject may also object to Processing for purposes of direct marketing, other than direct marketing by means of unsolicited electronic communications referred to in section 69 of POPIA.

¹¹ <https://inforegulator.org.za/popia-forms/>

¹² <https://inforegulator.org.za/popia-forms/>

Objections must be made on the POPIA Form 1.¹³

16.4 Right to withdraw consent (section 11(2)(b) of POPIA)

Where Processing is based on consent, the Data Subject may withdraw that consent at any time.

Withdrawal does not affect the lawfulness of Processing prior to the withdrawal.

16.5 Right not to be subject to automated decision-making (section 71) of POPIA)

A Data Subject has the right not to be subject, under certain circumstances, to a decision which results in legal consequences for him/her/it, or which affects him/her/it to a substantial degree, which is based solely on the automated processing of Personal Information intended to provide a profile of such person.

16.6 Right to lodge a complaint

A Data Subject has the right to submit a complaint to the Regulator regarding any alleged interference with the protection of Personal Information, as set out in clause 19, below.

17. Direct Marketing

17.1 Electronic direct marketing (section 69 of POPIA)

The Processing of Personal Information of a Data Subject for the purpose of direct marketing by means of any form of electronic communication, including automatic calling machines, facsimile machines, SMSs or email, is prohibited unless the Data Subject:

- Has given his, her or its consent to the Processing (opt-in); or
- Is, subject to subsection (3) of section 69 of POPIA, a Client of the Company.

¹³ <https://info regulator.org.za/popia-forms/>

The Company may approach a Data Subject (who is not an existing Client) only once for purposes of obtaining consent in the prescribed manner, by way of POPIA Form 4¹⁴ and only if the Data Subject has not previously withheld consent.

Where the Data Subject is an existing Client, the Company may only Process the Client's Personal Information for direct marketing of its own similar products or services if the Personal Information was obtained in the context of the sale of a product or service, the Data Subject was given a reasonable opportunity to object to such use at the time the information was collected, and on each marketing communication if the Data Subject did not initially refuse such use.

17.2 Other direct marketing

Direct marketing by other means (including post or in-person) is permitted, but the Data Subject has the right to object to such Processing at any time, free of charge and without having to provide reasons. Each marketing communication will provide a clear opt-out mechanism.

17.3 Suppression list

The Company maintains a suppression list of Data Subjects who have objected to direct marketing or withdrawn consent. The list is consulted before each direct marketing campaign.

18. Automated Decision-Making

The Company will not subject a Data Subject to a decision which results in legal consequences for him/her/it, or which affects him/her/it to a substantial degree, that is based solely on the automated Processing of Personal Information intended to provide a profile of such person, unless one of the exceptions in section 71(2) of POPIA applies:

- Where the decision is taken in connection with the conclusion or execution of a contract and the request of the Data Subject has been met (or appropriate measures have been taken to protect the Data Subject's legitimate interests); or

¹⁴ <https://info regulator.org.za/popia-forms/>

- Where the decision is governed by a law or code of conduct in which appropriate measures are specified for protecting the legitimate interests of Data Subjects.

Where automated decision-making is used, the Data Subject must be provided with sufficient information about the underlying logic of the automated Processing of Personal Information relating to him/her/it to be able to make representations.

19. Complaints

19.1 Internal complaints

Any Data Subject who is of the view that the Company has interfered with the protection of his/her/its Personal Information may lodge a complaint with the Information Officer at the contact details in clause 4, above.

The Information Officer will acknowledge receipt within 7 (seven) days and will investigate and respond to the complaint within 30 (thirty) days of receipt.

19.2 Complaints to the Regulator

A Data Subject may also, in terms of section 74 of POPIA, lodge a complaint with the Information Regulator alleging interference with the protection of Personal Information.

Complaints to the Regulator must be made on POPIA Form 5¹⁵ and submitted to the contact details in clause 23.

¹⁵ <https://info regulator.org.za/popia-forms/>

20. Training, Awareness and Compliance Monitoring

- All new Employees receive POPIA training as part of their induction.
- All Employees receive refresher POPIA awareness training at least once annually.
- Employees in functions with elevated privacy risk receive role-specific training.
- The Information Officer monitors compliance with this Policy through periodic reviews, audits and spot checks. **-set out actual dates**
- The Information Officer reports on POPIA compliance to the Directors at least annually.

21. Roles and Responsibilities

Directors	Approve this Policy; provide oversight; ensure adequate resources are allocated to compliance.
Information Officer	Oversees POPIA compliance; manages Data Subject requests; liaises with the Regulator.
Deputy Information Officer	Assists the Information Officer; acts in his/her absence.
Heads of Department/Managers	Implement this Policy in their areas; identify Processing activities; ensure that staff are trained.
IT (External)	Implements technical safeguards; supports incident response.
Human Resources	Manages Employee Personal Information; integrates POPIA into employment lifecycle.
Legal / Compliance	Reviews contracts (including Contractor agreements); supports the Information Officer.
All Employees, Contractors and Agents	Comply with this Policy; report incidents and concerns; complete required training.

Set Sail Claims Consultants (Pty) Ltd
POPIA Policy
01 July 2025
Version 1

22. Policy Review

This Policy is reviewed by the Information Officer at least annually, and on any material change to POPIA, the Regulations, guidance issued by the Regulator, or the Company's Processing activities.

Material amendments are approved by the Director(s) before publication.

23. Information Regulator Contact Details

The Information Regulator (South Africa) may be contacted at:

Physical address	Woodmead North Office Park, 54 Maxwell Drive, Woodmead, Johannesburg.
Postal address	P.O. Box 31533, Braamfontein, Johannesburg, 2017
Telephone (landline)	010 023 5200
Toll-free	0800 017 160
General enquiries	enquiries@inforegulator.org.za
POPIA complaints	POPIAComplaints@inforegulator.org.za
PAIA complaints	PAIAComplaints@inforegulator.org.za
Information Officer registration	IO@inforegulator.org.za
Website / eServices Portal	https://inforegulator.org.za https://eservices.inforegulator.org.za