DATA PROTECTION AND PRIVACY POLICY

SHIELD LIFE® LTD

(*"the Company"*)

Introduction

It is Shield's policy to protect the privacy and information of all its stakeholders.

Purpose

Shield is dedicated to the fundamentals of protecting consumer privacy and as such has created this Data Protection and Privacy Policy ("Policy") to standardise information privacy and data protection practices across all its business operations.

This Policy sets out how Shield Life Ltd (hereinafter referred to as "Shield") operates in South Africa and uses and protects the Personal Information (defined in *Definitions*) that it collects, stores, processes and disseminates from and to its Data Subjects (defined in *Definitions*).

This Policy also regulates the governance structure and implementation framework for the processing of such Personal Information.

Scope and Application

This Policy must be adhered to by:

- all employees, directors, officers and other staff of Shield ("Shield's Personnel"); and
- all third parties who Process the Personal Information of Shield's Data Subjects on behalf of Shield or as part of any functions or duties which they carry out (whether contractual or otherwise) for Shield ("Authorised Third Parties").

Shield employees are specifically referred to in sub-section *Employee use* and section *Disclosure* of this Policy, which deals with employee non-compliance with this Policy.

For the avoidance of any doubt, any reference to "Shield" in this document is to be considered a reference to Shield including but not limited to its Personnel and stakeholders, unless the context indicates otherwise.

This Policy is applicable to the processing of all Personal Information throughout the information life cycle, from the point of first collection of Personal Information until the time that such information is destroyed.

Definitions

Terms used in this policy:

"Child"	Means a person under the age of 18 (eighteen).
"Data Subject"	Means all persons whose Personal Information Shield and/or the Authorised Third Parties Processes, including all customers, employees, shareholders, suppliers, service providers and any other natural or juristic persons.
"Personal Information"	Means information (whether oral, written or in electronic form) relating to any Data Subject, including but not limited to (i) views or opinions of another individual about the Data Subject; and (ii) information relating to such Data Subject's i. race, sex, gender, sexual orientation, pregnancy, marital status, nationality, ethnic or social origin, colour, age, physical or mental health, well-being, disability, religion, conscience, belief, cultural affiliation, language and birth; ii. education, medical, financial, criminal or employment history; iii. names, identity number and/or any other personal identifier, including any number(s), which may uniquely identify a data subject, account or client number, password, pin code, customer code or number, numeric, alpha, or alpha-numeric design or configuration of any nature, symbol, e-mail address, domain name or IP address, physical address, cellular phone number, telephone number or other particular assignment; iv. blood type, fingerprint or any other biometric information; v. personal opinions, views or preferences; vi. correspondence that is implicitly or expressly of a personal, private or confidential nature (or further correspondence that would reveal the contents of the original correspondence); and vii. corporate structure, composition and business operations (in circumstances where the Data Subject is a juristic person) irrespective of whether such information is in the public domain or not.
"Privacy Officer"	Means the Shield Privacy Officer, who can be contacted at mail to: privacy@shieldlife.co.za
"Process, Processing"	Means any operation or activity or any set of operations concerning Personal Information, whether automated or not and including: i. the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use; ii. dissemination by means of transmission, distribution or making available in any other form by electronic communications or other means; or iii. merging, linking, blocking, degradation, erasure or destruction.
"PoPI Act"	The Protection of Personal Information Act No 4 of 2013 (South African Legislation).
"Special Personal Information"	Means information concerning a Data Subject's religious, spiritual or philosophical beliefs, race or ethnic origin, trade union membership, political opinions, physical or mental health, biometric information, sexual life, or criminal behaviour of a data subject to the extent that such information relates to alleged commission of any offence or any proceedings in respect of any offence allegedly.

Shield's Privacy Commitments

Shield has adopted the following five data privacy principles, on which this Policy is based:

1. OPENNESS AND HONESTY

   Shield should communicate honestly about any action that may impact on Data Subject Personal Information and privacy.

2. CHOICE

   Data Subjects should be given the options to make meaningful decisions about their Personal Information and privacy.

3. PRIVACY BY DESIGN

   Respect for Personal Information and privacy is and should be a critical element in the design, development and delivery of products and services by Shield.

4. LAWS AND STANDARDS

   Shield is committed to comply with all privacy laws and regulations applicable in South Africa and all countries in which it operates.

5. ACCOUNTABILITY

   Shield is accountable for adhering to the privacy principles set out in this Policy in all its business dealings.

Policy Objective

Data protection is of high strategic risk for Shield as Shield's failure to comply with its legal obligations to protect its Data Subjects' privacy and Personal Information could have repercussions (such as fines and penalties being imposed on Shield) and could result in Shield suffering reputational harm.

In South Africa, the PoPI Act has been enacted to regulate the processing of Personal Information.

In order to address these risks and legislative requirements, Shield will be responsible to implement and maintain systems and measures to ensure the protection of the privacy and Personal Information of all Data Subjects across all Shield businesses.

This also means that all Shield products and services must be in compliance with these requirements.

Data Protection Principles

The Processing of Personal Information by Shield and/or Authorised Third Parties must adhere to the following key principles, which are elaborated on in section *Application of Data Protection Principles* below:

Principle	Explanation
Legality	The Processing must be lawful and should be carried out in a reasonable manner and should not be excessive.
Purpose specification	The Processing must be for a specific and explicitly defined purpose.
Further processing limitation	Any further Processing of Personal Information must be compatible with the purpose for which it was collected (i.e. if Shield and/or any Authorised Third Party wishes to Process any Personal Information outside of the stated purpose for which it was collected).
Quality	The information processed must be complete, accurate and where necessary, kept updated.
Openness	The Data Subject must be made aware of the Processing.
Security	The integrity and confidentiality of the Personal Information must be ensured.
Data Subject participation	The right of the Data Subject to access their Personal Information and where necessary request correction or deletion of the Personal Information should be guaranteed.

Special Personal Information and Sensitive Information

Shield and/or Authorised Third Parties will not Process any Special Personal Information unless there is a compelling reason to do so and, in such cases, such Processing will only take place with the express permission of the Privacy Officer and in accordance with the provisions of the below.

Shield and/or Authorised Third Parties will only Process Special Personal Information listed in section *Data Protection Principles* to another person when:

- the consent of the Data Subject has been obtained;
- directed by an order of a court;
- it is necessary to disclose such information in order to provide products and services to the Data Subject (who is already a customer of Shield); or
- required in terms of any applicable law.

Shield and/or Authorised Third Parties may not Process any Personal Information concerning a Child and will only do so where it has obtained the consent of the parent or guardian of that Child or where Shield is permitted to do so in accordance with applicable laws.

In the event that Shield obtain or is requested to process Personal Information concerning a Child it will ensure all reasonably practicable steps have been taken to ensure the Privacy of the Child is protected.

The Implementation Framework

1. RESPONSIBILITY OF EACH BUSINESS UNIT

   All Shield business units are required to implement the provisions of this Policy.

2. WORK WITH THE PRIVACY OFFICER

Each Shield business unit and the Authorised Third Parties shall work through the office of the Privacy Officer as the first point of contact in its implementation of and ongoing compliance with this Policy.

3. MAINTAIN PERSONAL INFORMATION LOCATION REGISTER

In order to ensure effectiveness of privacy control measures it is essential that Shield knows where its Personal Information is stored. To this end, each business unit that Processes Personal Information must maintain a separate, up-to-date Personal Information location register to ensure effective management of all Personal Information Processed by that business unit.

4. MAINTAIN PRIVACY RISK REGISTER

In order to monitor and manage privacy risks across Shield, a Privacy Risk Register (recording all identified high privacy risks) must be maintained by all departments and business units, in which all identified risks affecting their respective departments are recorded. In this regard the register will, amongst other things, identify the risk in question, background to the risk and context, concerns and issues, steps taken to mitigate the risk and the person tasked with mitigating the identified risk.

5. PRIVACY RISK IMPACT ASSESSMENT

All business units that process Personal Information must, in consultation with the Privacy Officer, identify, prioritise and conduct regular privacy impact assessments, which serves as an important tool for providing relevant metrics relating to risks that need to be addressed and offering a methodology for prioritizing the manner in which risks will be addressed.

6. ALL SHIELD PRODUCTS AND SERVICES MUST COMPLY WITH THIS POLICY

All Shield Personnel and any Authorised Third Parties must adhere to this Policy and any other policies that govern privacy and the protection of Personal Information when developing products and rendering services, by identifying any privacy risks that might be posed by the product and/or service to be developed and by putting in place processes to mitigate these identified risks. Shield must ensure that relevant contracts are in place when doing business with any Authorised Third Party that processes personal information to comply with this policy.

Application of Data Protection Principles

1. PURPOSE SPECIFICATION AND CONSENT

Shield needs to ensure that they make Data Subjects aware of the fact that they are Processing their Personal Information and the purpose for which Shield will be Processing such Personal Information, including making the Data Subject aware of any Authorised Third Parties who may have access to the Personal Information (which may also include cross border transfers of Personal Information upon which Shield shall ensure that the privacy laws of such country is complied with). This obligation will also apply to Authorised Third Parties who collect Personal Information directly from a Data Subject.

Shield and/or Authorised Third Parties must always collect Personal Information in a fair, lawful and reasonable manner to ensure that it protects the Data Subject's privacy and Processes the Personal Information based on legitimate grounds in a manner that does not adversely affect the Data Subject(s) in question.

Where Shield and/or Authorised Third Parties collect Personal Information directly from the Data Subject and/or from third parties, and where Shield obtains Personal Information from third parties, Shield (or the Authorised Third Parties, where applicable) must ensure that it obtains the consent of the Data Subject to do so or only Processes the Personal Information without the Data Subject's consent where Shield is permitted to do so in terms of applicable laws.

Shield and/or Authorised Third Parties must obtain the Data Subject's consent prior to collecting, and in any case, prior to using or disclosing the Personal Information, unless such consent is not required, as approved by the Privacy Officer. The method of obtaining consent and/or confirming consent should also be approved by the Privacy Officer.

The Data Subject may withdraw his/her consent or object to Shield's processing of the Personal Information at any time. If the consent is withdrawn or if there is otherwise an objection against the use of or the processing of such Personal Information, Shield and/or the Authorised Third Parties must ensure that the Personal Information is no longer Processed and that the Privacy Officer is advised of each such instance of withdrawal or objection to the provision of consent. Request with reason for withdrawal may be sent to privacy@shieldlife.co.za

All withdrawn consent and/or objection against the use of or processing of personal information shall be stored in a centralized database.

Shield and/or the Authorised Third Parties must only Process Data Subject Personal Information for a specific, lawful and clear purpose and as set out in the first paragraph of this section and must ensure that it makes the Data Subject aware of such purpose(s) as far as possible. Shield will ensure that the necessary consent to the Processing of any Personal Information will relate only to the purpose for which the Data Subject has been made aware of and Shield and/or the Authorised Third Parties will not Process any Personal Information for any other new purposes which the Data Subject has not consented to.

A record of the Data Subject's consent will be required as confirmation or acknowledgement by the Data Subject that Shield may use the Personal Information for one or more of the following purposes:

- For the purpose of Shield providing any services or products to the Data Subject from time to time;
- For the purposes of receiving services or products provided by the Data Subject to Shield from time to time;
- If a Data Subject is an employee, in the course and scope of employment by Shield;
- To respond to any correspondence that the Data Subject may send to Shield, including via e-mail or by telephone;
- To contact the Data Subject from time to time, where specific consent has been given to follow-up contacts by Shield or to be put on Shield's mailing list;
- For such other purposes to which the Data Subject may consent from time to time; and
- For such other uses authorised in terms of applicable law.

2. KEEPING PERSONAL INFORMATION ACCURATE

Shield and/or Authorised Third Parties must ensure that all Personal Information is kept as accurate, complete and up-to-date as far as possible and must implement appropriate system/s to manage this.

Shield may not always expressly request the Data Subject to verify and update his/her Personal Information, unless this process is specifically necessary or the circumstances under which Shield engages with the Data Subject allows for such request to be made. As a general principle, all Personal Information should be kept up to date, unless the Privacy Officer has provided written permission that same is not required in specific circumstances.

The Data Subjects are entitled to notify Shield from time to time of any updates required in respect of their Personal Information and to this end, Shield and the Authorised Third Parties will provide a centralized procedure through which Data Subject details can be updated.

3. SECURITY MEASURES AND SECURITY BREACH INCIDENTS

Shield and Authorised Third Parties are required to implement and maintain physical, organisational, contractual and technological security measures to keep all Personal Information secure, including protecting any Personal Information from loss or theft, and unauthorized access, disclosure, copying, use or modification.

Shield is required to adhere to the relevant security policies (listed in the Cyber Risk and Security Policy, as amended from time to time) for protecting Personal Information (both logically and physically).

Compliance with these security measures and safeguards does not guarantee that an appropriate level of protection is provided for purposes of this Policy and therefore the security measures will be re-assessed on a regular basis as information security techniques and the threats to security evolve and new risks are identified. This includes identifying all reasonably foreseeable risks and establishing and maintaining appropriate safeguards to address these risks on an on-going basis.

Shield's Technology team shall carry out holistic and comprehensive assessments and verification to ensure that the security safeguards have been effectively implemented within Shield.

Shield's Technology team will be responsible for the day to day maintenance of all relevant systems to ensure the protection of Personal Information stored and/or Processed on these systems.

Each business unit within Shield is expected to put in place systems to respond to security breaches or data loss incidents which ensures that:

- the business impact of each incident will be identified;
- Shield's reputation is protected where a fast and effective response is delivered;
- corporate liability due to lack of due diligence is mitigated; and
- regulatory requirements are met, including any relevant statutory obligations to report data losses to the Information Regulator and/or Data Subjects who might be affected. Where this is required, Shield will notify any affected Data Subject(s) and the Information Regulator in writing in the event of a security breach (or a reasonable belief of a security breach) in respect of any Data Subject Personal Information, via the office of the Privacy Officer. Shield must provide such notification as soon as reasonably possible after it has become aware of any security breach of Personal Information.

4. AUTHORISED THIRD PARTIES' PROCESSING PERSONAL INFORMATION

Personal Information will only be provided to Authorised Third Parties (including where such Authorised Third Parties host or Process or access Personal Information on Shield's systems) where consent is obtained from the Data Subjects in question or in furtherance of a business need or in compliance with a legal obligation. The extent of the consent required will be determined in consultation with the Privacy Officer.

Where necessary or appropriate, agreements with Authorised Third Parties to whom Shield may disclose Personal Information must be concluded to ensure that they Process any Personal Information in accordance with the provisions of this Policy and the relevant laws. All such Authorised Third Parties should at the very least conclude non-disclosure agreements containing data protection provisions with Shield compelling them to treat all Personal Information in their possession as confidential and preventing such third parties from disclosing such information.

All Authorised Third Parties who Process Data Subject Personal Information must strictly adhere to the security requirements set forth in this Policy and to Shield's security policies (listed in Cyber Risk and Security Policy, as these are amended from time to time) and shall be required to maintain and where required, upgrade their systems and processes to comply with the terms of this Policy and such security policies.

Shield should carry out a due diligence of all Authorised Third Parties Processing Personal Information on behalf of Shield and this may include reviewing the facilities of such Authorised Third Parties Where Personal Information hosted by Authorised Third Parties falls into a medium or high risk category of sensitive information as described in section *Special Personal Information and Sensitive Information* hereto, which determination shall be carried out by the Chief Information Officer.

Authorised Third Parties must immediately inform Shield (via the office of the Privacy Officer) of any actual or suspected security breach or compromise to Personal Information in its possession. The Authorised Third Parties may be required to notify the affected Data Subject(s) and the Information Regulator, but this should only be carried out on Shield's instructions, via the office of the Privacy Officer.

5. USE OF PERSONAL INFORMATION FOR DIRECT MARKETING PURPOSES

Shield can use Personal Information in its possession for direct marketing purposes by means of any form of electronic communication if the Data Subject has consented to such use. The manner and procedure for recording the consent obtained in this regard shall be approved by the Privacy Officer.

Where no consent was obtained from the Data Subject, the use of Personal Information for direct marketing purposes is subject to ALL of the following conditions:

- The information ought to have been obtained in the context of the sale of goods or services;
- It must be used to market Shield's own similar products or services; and
- The Data Subject must be given a reasonable opportunity to opt out, either when the information is or was originally collected and/or (if the Data Subject has not initially refused or opted out of such use) on occasion of each direct marketing communication.

The direct marketing communication must contain Shield's details or details of the third party who sends the communication on behalf of Shield; and the contact details to which the recipient of the message can send an opt-out request.

Any deviation from the above position must be approved by the Compliance Departments in consultation with the Privacy Officer.

6. DATA SUBJECT ACCESS TO INFORMATION

Data Subjects are entitled to request written confirmation that Shield holds his/her/its Personal Information and to request that Shield furnishes a description thereof. Any such requests shall be dealt with via the office of the Privacy Officer and, in the case of South Africa, in accordance with Shield's PAIA Manual (located at http://www.shieldlife.co.za/Content/uploads/PAIA.pdf, and issued in terms of the Promotion of Access to Information Act 2 of 2000) and this Policy. Shield will provide the Data Subject with any such Personal Information to the extent required by law and in terms of the Promotion of Access to Information Act 2 of 2000. Shield may, in certain cases, refuse to grant the requested access to information.

In the case of Shield, Data Subjects may challenge the accuracy or completeness of their Personal Information in Shield's records at any time through the process set out under Shield's PAIA Manual for accessing information.

If a Data Subject successfully demonstrates that their Personal Information in Shield's records is inaccurate or incomplete, Shield must ensure that such Personal Information is amended or deleted as required (including by any Authorised Third Parties).

7. DATA STORAGE AND RETENTION

Shield and Authorised Third Parties must ensure that Personal Information, Special Personal Information and any commercially sensitive information which it Processes is stored, captured, used, disclosed and destroyed in a secure and confidential manner appropriate to the classification of the information, in accordance with the Shield Data Retention and Destruction Policy.

Shield must keep the Personal Information that it Processes on behalf of Data Subjects at its various business sites an in line with operating procedures determined by technology department.

Authorised Third Parties, including data storage and processing providers, may from time to time also have access to a Data Subject's Personal Information in connection with the storage and retention thereof. Shield will ensure that these Authorised Third Parties will Process the Personal Information in accordance with the provisions of this Policy, all other relevant internal Shield policies and the PoPI Act.

As is further detailed in Shield's document retention policy, the following is applicable:

- Shield may keep records of the Personal Information it has collected, correspondence or comments in an electronic or hardcopy file format. Personal Information may be processed for as long as necessary to fulfil the purposes for which that Personal Information was collected and/or as permitted or required by applicable law.
- Shield may retain Personal Information for longer periods for statistical, historical or research purposes, and should this occur, Shield must ensure that appropriate safeguards have been put in place to ensure that all recorded Personal Information will continue to be Processed in accordance with this Policy and the applicable laws.
- Once the purpose for which the Personal Information was initially collected and Processed no longer applies or becomes obsolete, Shield will ensure that it is deleted, destroyed or de-identified, so that a third party cannot re-identify such Personal Information.

8. CROSS BORDER DATA TRANSFERS

Shield can send or transfer Personal Information of Data Subjects to Authorised Third Parties beyond the borders of the countries in which Personal Information is collected in order to achieve the purpose for which the Personal Information was collected and Processed, including for Processing and storage by Authorised Third Parties, if the applicable Data Subject(s) has consented to such cross-border transfer.

Where no consent has been obtained, the cross-border transfer must meet one of the following conditions (as approved by the Privacy Officer):

- The recipient must be subject to existing legislation in his /her/its country or to binding corporate rules or to a binding agreement that enforces and upholds Personal Information protection measures which are acceptable to Shield;
- The transfer must be necessary for the conclusion and/or performance of a contract between Shield and the Data Subject;
- The transfer must be necessary for the conclusion or performance of a contract entered into, in the interest of the Data Subject, between Shield and the relevant group company or the Authorised Third Party; and

- The transfer must be to the benefit of the Data Subject and must take place in circumstances under which it is not reasonably possible to obtain the Data Subject's consent and where it is reasonably possible to obtain such consent; the Data Subject would be likely to give it.

The processing of Personal Information in a foreign jurisdiction may be subject to the laws of the country in which it is held, and may be subject to disclosure to the Governments, Courts of law, Enforcement or Regulatory Agencies of such other country, pursuant to the laws of such country.

Processing of Shield Personnel Personal Information

Shield's HR function shall ensure that they comply with this Policy is respect of all Shield Personnel data which they have on file and collect, and which falls within the definition of Personal Information, including that HR will only collect such Personal Information of its employees as is necessary for their employment relationship with Shield. This includes information collected from the time that a potential employee applies for a job, during the interview and selection process and if such candidate is successful, all information processed during the course of their employment and on the termination of their employment.

The appropriate consent forms should be included as part of the terms of engagement and/or employment contracts concluded with each of the Shield Personnel (including employees, temporary employees, independent contractors, consultants, etc.).

Disclosure

1. EMPLOYEE USE

   Shield Personnel entrusted with the custody of Processing Personal Information in the course of their duties may only use such information in pursuit of their duties and for the purpose for which it is collected and for no other reason whatsoever. Any failure to comply with this requirement could result in disciplinary action and possible dismissal.

2. DISCLOSURE OF PERSONAL INFORMATION TO LAW ENFORCEMENT AND/OR JUDICIAL AUTHORITIES

   Shield is required to provide Personal Information to law enforcement agencies and/or to judicial authorities in terms of various applicable laws. These requests or instructions are typically in the nature of court orders, subpoenas, warrants and or other judicial / law enforcement processes. Any such requests should be routed via the Privacy office.

3. INTERGROUP DISCLOSURES

   Any disclosure of Personal Information between the Group of companies must be carried out in compliance with the terms of this Policy, including as regards having obtained appropriate consents from the Data Subjects in question which allows for such intergroup disclosure. Provided that such disclosure complies with the terms of this Policy and any applicable laws, all Group companies who Process Data Subjects' Personal Information must ensure that it only Processes such Personal Information within the 'purpose specification' and for no other purposes.

Policy Violations

Non-compliance with this Policy constitutes misconduct and could, in the case of employees of Shield, result in disciplinary action in terms of Shield's Disciplinary Procedure and Code and could lead to dismissal and/or further legal action being taken against the responsible Shield employee(s).

Responsibility

The Chief Information Officer is responsible for ensuring that this Policy is accepted and implemented throughout Shield.

The Chief Executive Officer of Shield is in turn responsible for verifying that the company and its operations in the relevant local market, comply with this Policy.

A governance structure has been implemented to manage the risks associated with Shield's Processing of Personal Information, which is set out in section *Governance Structure and Processes* hereto. The respective committees will be engaged on privacy related matters depending on the degree of risk categorization assigned to the matter at hand.

Monitoring and Review

This Policy will be reviewed at regular intervals when appropriate and in accordance with Shield's Privacy Management System.

Governance Structure and Processes

The following governance structure applies to Shield managing the implementation and application of this Policy:

Privacy Core Team:

Position	Roles and Responsibilities
Chief Executive Officer	Is the ultimate custodian of Personal Information across Shield.
Chief Risk Officer	Identify risks across Shield and recommend mitigation measures.
Chief Information Officer	• Implement the necessary security measures and technologies to protect Personal Information during Processing within Shield. • Implement technical and other measures – when required – to mitigate information security risks. • Manage all data breach incidents and related reporting.
Privacy Officer	• Oversee the implementation of this Policy across Shield. • Escalate all matters relating to this Policy and other privacy issues to the Executive Sponsor.

The Privacy Forum:

The privacy forum is responsible for coordinating, monitoring and ensuring compliance with all privacy and security policies across Shield. In this regard the Privacy Forum is responsible for:

- Ensuring alignment of operational activities relating to privacy and security
- Reviewing privacy policies annually or when the need arises
- Monitoring the privacy and data protection practices across Shield
- Acting as the risk escalation body for privacy and security issues
- Ensuring consistent communication and raising awareness across Shield about privacy issues
- Identifying and reviewing identified privacy incidents

The Privacy Forum is comprised of the Privacy Officer and representatives from Technology and Risk Management.