Golden Pond Trading 616 (Pty) Ltd t/a Independent Trustee Services

Protection of Personal Information Policy

1. Scope

This policy applies to everyone with access to Personal Information available to them due to their relationship with Independent Trustee Services.

It addresses the rights of Data Subjects, being the various categories of people whose personal information we have access to.

Personal Information broadly means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly to a specific natural or juristic person / Data Subject.

This policy must be read together with Independent Trustee Services' Records Management, Cyber Security and Business Continuity Policies.

2. Purpose

This Policy aims to ensure Independent Trustee Services' compliance with various laws and regulations addressing Personal Information and sets out how Independent Trustee Services handles their Data Subjects' Personal Information and additionally lists the purpose(s) said information is used for.

3. Policy

Independent Trustee Services is committed to protecting the privacy of Data Subjects and to ensuring that their Personal Information is used appropriately, transparently, securely and in accordance with applicable laws.

We subscribe to the Protection of Personal Information Act Principles and will:

1. Obtain and process information fairly.
2. Keep information only for one or more specified, explicit, and lawful purposes.
3. Use and disclose information only in ways compatible with these purposes.
4. Keep information safe and secure.
5. Keep information accurate, complete, and up to date.
6. Ensure that information is adequate, relevant, and not excessive.
7. Retain information for no longer than is necessary for the purpose or purposes.
8. Provide a copy of personal data kept to the Data Subject on request.

4. Procedures

4.1 Personal Information Collected

Independent Trustee Services will generally collect some of the following personal information from our Data Subjects:

- Information relating to the race, gender, sex, pregnancy, marital status, national, ethnic, or social origin, colour, age, physical or mental health, well-being, disability, language, and birth.
- Information relating to the education, medical, financial, criminal or employment history.
- Identifying number, name, symbol, e-mail address, physical address, telephone number, location information.
- Biometric information (employees).
- Correspondence sent/received 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 our Data Subject.

We have agreements in place with all our product suppliers, and third-party service providers to ensure that there is a mutual understanding with regards to the protection of Personal Information.

We may also supplement the information provided with information we receive from other providers to offer a more consistent and personalised experience in clients' interaction with us.

4.2 How Personal Information is used

Personal Information will only be used for the purpose for which it was collected and agreed. This may include:

- Providing a product / service to a Data Subject;
- As part of employee on-boarding or any other internal human resources function;
- Conducting credit reference searches or verification;
- Confirming, verifying, and updating contact details;
- For the detection and prevention of fraud, crime, money laundering or other malpractice;
- For audit and record keeping purposes;
- In connection with legal proceedings;
- Providing our services to a Data Subject to carry out the services requested and to maintain and constantly improve the relationship;
- Providing communications in respect of INDEPENDENT TRUSTEE SERVICES and regulatory matters that may affect Data Subjects;
- In connection with and to comply with legal and regulatory requirements or when it is otherwise allowed by law;
- To carry out the transaction(s) requested;
- For underwriting purposes;
- Assessing and processing claims;
- For purposes of claims history; and or
- Conducting market or customer satisfaction research.

In terms of the provisions of the Protection of Personal Information Act, Personal Information may only be processed if certain conditions are met, which are listed below, along with supporting information for Independent Trustee Services processing of Personal Information:

- When Data Subject consents to the processing – consent only required where the information will be used for something other than the intended use for which the information is supplied.
- The processing is necessary.
- Processing complies with an obligation imposed by law on Independent Trustee Services.
- Processing protects the legitimate interest of the Data Subject.
- Processing is necessary for pursuing the legitimate interest of Independent Trustee Services or of a third party to whom information is supplied.

4.3 Disclosure of Personal Information

We will only disclose a Data Subject's Personal Information for a reason it was not intentionally supplied for where we have a duty or a right to disclose in terms of the law or where it is necessary to protect our rights.

We have agreements in place to ensure compliance with confidentiality and privacy conditions.

We may also share client Personal Information with, and obtain information about, clients from third parties for the reasons already discussed above.

4.4 Safeguarding Personal Information

We will adequately protect the Personal Information we hold and avoid unauthorised access and use of Personal Information. We will continuously review our security controls and processes to ensure that personal Information is secure.

When we contract with third parties, we impose appropriate security, privacy, and confidentiality obligations on them to ensure that Personal Information is kept secure.

We may need to transfer (electronic) Personal Information to another country for processing or storage. We will ensure that anyone to whom we pass personal information agrees to treat Personal Information with a similar level of protection as afforded by ourselves.

4.5 Access and correction of Personal Information

Data Subjects have the right to access the Personal Information we hold about them. Data Subjects also have the right to request us to update, correct or delete their Personal Information on reasonable grounds. Once a Data Subject objects to the processing of their Personal Information, Independent Trustee Services may no longer process said Personal Information. We will take all reasonable steps to confirm our Data Subject's identity before providing details of their Personal Information or making changes to their Personal Information. Independent Trustee Services' Information Officer will be responsible for managing this process.

4.6 Data breaches

Even though Independent Trustee Services will take every precaution to prevent a data breach, a breach may still occur.

A personal data breach is a breach of security leading to a:

- Confidentiality breach – an accidental or unauthorised disclosure of, or access to, personal data.
- Availability breach – an accidental or unauthorised loss of access to, or destruction of, personal data and/or
- Integrity breach – an accidental or unauthorised alteration of personal data.

4.6.1 Notification to the Information Regulator ("IR")

The Information Regulator must be notified of the breach if it is likely to result in a risk to the rights and freedoms of data subjects i.e., if, for example, it could result in:

- loss of control over their data
- limitation of their rights
- discrimination
- identity theft
- fraud
- damage to reputation
- financial loss
- unauthorised reversal of pseudonymisation
- loss of confidentiality
- any other significant economic or social disadvantage.

Where a breach is reportable, the Company must notify the Information Regulator without undue delay and, where feasible, no later than 72 hours after becoming aware of the breach. If our report is submitted late, it must also set out the reasons for our delay.

The notification must at least include:

- a description of the nature of the breach including, where possible, the categories and approximate number of affected data subjects and the categories and approximate number of affected records;
- the name and contact details of the **Information Officer**;
- a description of the likely consequences of the breach; and
- a description of the measures taken, or to be taken, by the Company to address the breach and mitigate its possible adverse effects.

4.6.2. Communication to affected Data Subjects

Where the personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, Independent Trustee Services also needs to communicate the breach to the affected data subjects without undue delay, i.e., as soon as possible.

Reporting to Data Subjects may however be delayed if reporting may lead to an increased risk to the Data Subject.

In clear and plain language, Independent Trustee Services must provide affected Data Subjects with:

- a description of the nature of the breach;
- the name and contact details of Independent Trustee Services' Information Officer and CEO;
- a description of the likely consequences of the breach;
- a description of the measures taken, or to be taken, by Independent Trustee Services to address the breach and mitigate its possible adverse effects;
- practical advice on how to limit the damage, e.g., resetting their passwords; and
- Data subjects will be contacted individually, by e-mail, unless that would involve Independent Trustee Services in disproportionate effort such as where contact details have been lost as a result of the breach or were not known in the first place, in which case we will use a public communication, such as a notification on our website.

However, Independent Trustee Services is not required to report the breach to Data Subjects if:

- appropriate technical and organisational protection measures have been implemented, and those measures have been applied to the personal data affected by the breach, in particular those that render the personal data unintelligible to any person who is not authorised to access them, such as state-of-the-art encryption, or
- subsequent measures were taken to ensure that the high risk to the rights and freedoms of Data Subjects is no longer likely to materialise.

Communication to Data Subjects with regards to Data Breaches may under no circumstances be communicated or published without prior approval of Independent Trustee Services **Information Officer**.

4.6.3 Data breach register

Independent Trustee Services will maintain a register of all personal data breaches, regardless of whether they are notifiable to the Information Regulator.

4.6.5 Data breach reporting procedure

If anyone knows or suspects that a personal data breach has occurred, they must immediately both advise their line manager and contact the Company's CEO. Evidence in relation to the breach must be retained.

Independent Trustee Services will investigate and assess the actual or suspected personal data breach in accordance with the response plan set out below and will determine who should be notified and how.

4.6.6 Response plan

According to Independent Trustee Services' response plan the **Deputy Information Officer** will:

- Make an urgent preliminary assessment of what data has been lost, why and how.
- Take immediate steps to contain the breach and recover any lost data.
- Undertake a full and detailed assessment of the breach.
- Record the breach in the Company's data breach register.
- Notify the Information Regulator where the breach is likely to result in a risk to the rights and freedoms of data subjects.
- Notify affected Data Subjects where the breach is likely to result in a high risk to their rights and freedoms.
- Respond to the breach by putting in place any further measures to address it and mitigate its possible adverse effects, and to prevent future breaches.

Please see Annexure B for more information.

4.7 Information Officer and Deputy Information Officer

The Protection of Personal Information Act appoints the highest level of authority in an organisation as the Information Officer. The Information Officer has been tasked with ensuring compliance with data protection and privacy legislation and regulations.

The Information Officer has appointed a Deputy Information Officer to perform the required tasks.

The details of our Information Officer and Deputy Information Officer are as follows:

Information Officer
Name and Surname: Henry Dul
Information Officer Registration Number: 2024-011380

Deputy Information Officer
Name and Surname: Elizabeth Randles

Both our Information Officer and Deputy Information Officer are contactable at our Head Office:

Telephone Number:
011 675 2092

Physical Address:
1st Floor, Quadrum 1, Quadrum Office Park,
50 Constantia Boulevard,
Constantia Kloof, 1709

Email Address:
Information Officer: henry@its-mail.co.za
Deputy Information Officer: liz@its-mail.co.za

Website:
www.independenttrusteeservices.co.za

5. Consequences of Non-Adherence

Compliance monitoring will be performed regularly, and feedback will be provided to the **Information Officer** of Independent Trustee Services.
Action will be taken against those that do not adhere to requirements and principles stated in this policy.

5. Training and awareness

Relevant staff will receive training on what is required from them.

6. Review

This policy shall be reviewed as and when Independent Trustee Services' compliance management strategy and framework change or the business strategy changes, but at least annually.

7. Version control and approval

Version	Date approved	Approved by	Notes
	October 2024	Henry Dul	

Annexure B: Data Breach Response plan for INDEPENDENT TRUSTEE SERVICES

CONTAIN

- Data breaches must immediately on discovery be reported to the Information Officer who will drive implementation of this plan.
- If the breach took place through an electronic device:
  - Take the device offline immediately, but DO NOT shut it down
  - Change passwords

ASSESS

- Determine the extent of the breach
  - who was affected
  - which records have been affected
- Determine the impact of the breach
- Determine if the breach should be reported to
  - the Information Regulator
  - Data Subjects

MANAGE

- Agree what the appropriate actions will be
  - Facilitate technology restoration or recovery if applicable
  - Prepare and submit insurance claim
- Communicate decisions internally
- Prepare (and arrange for authorisation of) and Communicate with Customer(s) / Public
- Take remedial action to prevent similar breaches