GOVERNANCE • PRIVACY • INFORMATION SECURITY

PROTECTION OF PERSONAL INFORMATION POLICY

2026 EDITION

Golden Pond Trading 616 (Pty) Ltd
trading as Independent Trustee Services

Document control	Details
Policy owner	Information Officer
Version	2.0
Effective date	15/07/2026
Approval authority	Information Officer / governing body
Review cycle	At least annually and upon a material legal, operational or security change
Related documents	PAIA Manual; Records Management; Cybersecurity; Business Continuity; Incident Response

Policy status: This policy supersedes the October 2024 policy and becomes operative only after formal approval.

1. Purpose

Independent Trustee Services ("ITS", "we", "us" or "our") respects the constitutional right to privacy and is committed to processing personal information lawfully, reasonably, transparently and securely. This policy establishes the governance and operational controls used to comply with the Protection of Personal Information Act 4 of 2013 ("POPIA"), its regulations and applicable guidance, as well as the Promotion of Access to Information Act 2 of 2000 ("PAIA").

The policy is designed to protect data subjects, support fair and accountable client and employee outcomes, and enable ITS to demonstrate compliance. It must be read with the PAIA Manual, privacy notices, retention schedule, cybersecurity, records-management, business-continuity and incident-response controls.

2. Scope and application

This policy applies to all personal information processed by ITS in any form and to all directors, officers, employees, representatives, contractors, consultants and operators acting for ITS. It covers information relating to identifiable living natural persons and, where applicable under POPIA, identifiable existing juristic persons.

It applies across the information lifecycle: collection, receipt, recording, organisation, storage, updating, retrieval, consultation, use, dissemination, transfer, restriction, archiving, destruction and deletion. Contractual duties owed to retirement funds, clients or other responsible parties may impose additional controls.

3. Key roles and terminology

Term	Meaning
Responsible party	The person that, alone or with others, determines the purpose of and means for processing personal information. ITS may be a responsible party for its own operations and an operator when processing on documented instructions for a client.
Operator	A person that processes personal information for a responsible party under a contract or mandate without coming under the direct authority of that party.
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, as more fully defined in POPIA.
Special personal information	Information concerning religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, biometric information or criminal behaviour.
Processing	Any operation or activity concerning personal information, whether automated or not.
Security compromise	Circumstances where there are reasonable grounds to believe personal information has been accessed or acquired by an unauthorised person.

4. Governance and accountability

ITS remains accountable for compliance and must implement reasonable technical and organisational measures appropriate to the nature of the information, potential harm, available technology, cost and sector practices. The Information Officer oversees the compliance framework but every person processing information is responsible for complying with this policy.

ITS will maintain, as appropriate:

- a documented POPIA compliance framework and annual compliance plan;
- a personal-information inventory and processing register;
- privacy impact assessments for new, changed or high-risk processing;
- current privacy notices and consent records where consent is relied upon;
- operator due diligence and written operator agreements;
- a retention and secure-destruction schedule;
- data-subject request, objection and complaint registers;
- a security-compromise register and response capability; and

- training, monitoring, assurance and management reporting.

5. Conditions for lawful processing

Condition	ITS control
Accountability	Assign ownership, maintain evidence and monitor compliance throughout the processing lifecycle.
Processing limitation	Process lawfully and reasonably, without unjustifiably infringing privacy; collect only adequate, relevant and non-excessive information.
Purpose specification	Collect for a specific, explicitly defined and lawful purpose; communicate the purpose; retain only as long as authorised or necessary.
Further processing limitation	Ensure subsequent use is compatible with the original purpose unless POPIA permits otherwise.
Information quality	Take reasonably practicable steps to keep information complete, accurate, not misleading and updated where necessary.
Openness	Maintain documentation and provide section 18 notifications, subject to lawful exceptions.
Security safeguards	Identify risks and maintain appropriate, reasonable technical and organisational safeguards, including operator controls.
Data-subject participation	Enable access, correction, deletion and objection rights in accordance with POPIA and PAIA.

6. Lawful justification

Before processing begins, ITS must document at least one justification under section 11 of POPIA. Consent is not the only justification and must not be used where it is not voluntary, specific and informed. Processing may be justified where:

- the data subject or a competent person 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 ITS;
- 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 ITS or a third party, after balancing those interests against the data subject's rights and reasonable expectations.

ITS must be able to prove consent where relied upon. Consent may be withdrawn, without affecting prior lawful processing. A lawful objection under section 11(3) must be actioned and the relevant processing stopped unless another binding legal basis or exception lawfully applies.

7. Personal information processed and purposes

Depending on the mandate and relationship, ITS may process identification and contact details; financial, tax, employment, retirement-fund and benefit information; regulatory due-diligence information; correspondence; instructions; transaction and service records; complaints; supplier details; system and access logs; and employee information. Race, health, disability, biometric or criminal-behaviour information is processed only where specifically authorised and necessary.

Purposes may include client onboarding and service delivery; trustee, fiduciary and secretarial functions; retirement-fund administration support; identity and authority verification; FICA and other regulatory compliance; fraud and financial-crime prevention; billing, accounting and audit; legal claims; complaints; employment and supplier administration; security and business continuity; and communications reasonably connected with the relationship.

8. Collection and privacy notification

Personal information should be collected directly from the data subject unless POPIA permits indirect collection. Information may also be obtained from clients, employers, retirement funds, authorised representatives, public records, regulators, screening providers, service providers and other lawful sources.

At or before collection, or as soon as reasonably practicable thereafter, ITS must provide a clear section 18 privacy notification covering the information collected, source, responsible party, purpose, whether supply is voluntary or mandatory, consequences of failure, legal authority, recipients, cross-border transfers, data-subject rights, Information Officer details and the right to complain to the Information Regulator, subject to statutory exceptions.

9. Special personal information and children

Special personal information and information concerning children may be processed only where a general or specific authorisation under POPIA applies, or the Information Regulator has granted the necessary authorisation. Access must be limited to persons who require it for an authorised purpose, with enhanced confidentiality, monitoring, retention and security controls.

Prior to new or materially changed processing, the Information Officer must determine whether Regulator authorisation or prior authorisation is required under sections 27, 35 or 57–59 and must ensure that processing does not commence prematurely.

10. Health information: 2026 sector requirements

Because ITS works for or with retirement funds, employers and related bodies, the Regulations relating to the Processing of Data Subjects' Health Information by Certain Responsible Parties, 2026 apply where ITS processes health information within their scope. Health information must be processed only under a valid POPIA authorisation and subject to a duty of confidentiality imposed by law, office, employment, profession or written agreement.

ITS must maintain confidentiality, integrity and availability through sector-appropriate safeguards addressing physical and electronic records, access, transmission, storage, recovery and secure disposal. Health information may not be transferred outside South Africa unless one or more requirements in section 72(1) of POPIA are met. Where ITS acts as operator, it must also comply with the responsible party's lawful documented instructions and contractual safeguards.

11. Information quality, minimisation and records

Business owners must ensure that information is adequate, relevant and not excessive for the purpose, and take reasonably practicable steps to keep it complete, accurate, not misleading and updated where necessary. Data subjects and authorised sources should be used to validate material information. Corrections must be propagated to relevant records and recipients where appropriate.

12. Retention and secure destruction

Personal information must not be retained longer than authorised by law, required for the purpose, reasonably required by contract, or needed for lawful historical, statistical, research, evidential or litigation purposes with suitable safeguards. ITS will maintain a retention schedule aligned to FAIS, FICA, pension-fund, employment, tax, corporate, contractual and limitation requirements.

When retention is no longer justified, information must be destroyed or deleted in a manner that prevents reconstruction in an intelligible form. Legal holds, complaints, investigations and litigation must suspend ordinary destruction. Destruction must be controlled and evidenced, including when performed by an operator.

13. Security safeguards

ITS must identify reasonably foreseeable internal and external risks, establish and maintain safeguards, verify their effectiveness and update them as risks evolve. Controls should include, proportionate to risk:

- role-based access and least privilege; joiner, mover and leaver controls;
- multi-factor authentication, secure password management and privileged-access controls;
- encryption or equivalent safeguards for transmission, portable media and sensitive repositories;

- secure configuration, patching, malware protection and vulnerability management;
- logging, monitoring, backups, recovery testing and business continuity;
- physical access, clean-desk, secure printing and document-disposal controls;
- data-loss prevention and approved communication and storage channels;
- phishing awareness, confidentiality undertakings and periodic access reviews; and
- incident exercises, operator assurance and remediation tracking.

14. Operators and third parties

Before appointing an operator, ITS must assess its security, privacy capability, location, subcontracting and breach-management arrangements. A written contract must require the operator to process only with ITS's knowledge or authorisation, preserve confidentiality, establish and maintain section 19 safeguards, notify ITS immediately of reasonable grounds to suspect unauthorised access or acquisition, support rights requests and audits, control subcontractors and return or securely destroy information on termination.

Where ITS acts as operator for a client, ITS must process within the mandate and written instructions, escalate conflicting or unlawful instructions, support the responsible party's compliance and not use the information for an unauthorised independent purpose.

15. Cross-border transfers

ITS may transfer personal information to a third party in another country only where section 72 of POPIA permits it. The Information Officer must document that:

- the recipient is subject to a law, binding corporate rules or binding agreement providing an adequate level of protection;
- the data subject consents to the transfer;
- the transfer is necessary for performance of a contract with the data subject or pre-contractual measures requested by the data subject;
- the transfer is necessary for concluding or performing a contract in the data subject's interest; or
- the transfer benefits the data subject, consent is not reasonably practicable and the data subject would probably have consented.

Cloud hosting, remote support, backups and access from outside South Africa are transfers and must be assessed. Additional health-information, client-contract and confidentiality restrictions remain applicable.

16. Direct marketing and communications

Unsolicited electronic direct marketing must comply with section 69 and the Information Regulator's guidance. A non-customer may be approached only once to request compliant consent if that person has not previously withheld consent. Consent must be voluntary, specific, informed and recorded using Form 4 or a substantially similar mechanism.

Existing customers may be marketed similar products or services only where their details were obtained in the context of a sale or service and they received a free, simple opportunity to object when collected and in every communication. Communications must identify the sender, provide contact details and contain a functional opt-out. ITS will maintain consent and suppression records and must not contact an objector again for the affected marketing purpose.

17. Automated decision-making

ITS must not subject a data subject to a decision based solely on automated processing that produces legal consequences or substantially affects the person, unless section 71 permits it and appropriate measures protect legitimate interests. Those measures include an opportunity to make representations and sufficient information about the underlying logic. New automated decision tools require a privacy impact assessment and Information Officer approval.

18. Data-subject rights and request handling

Subject to POPIA, PAIA and lawful limitations, a data subject may request confirmation and access; request correction, destruction or deletion; object to certain processing; withdraw consent; object to direct marketing; and

complain to ITS or the Information Regulator. Prescribed Forms 1 and 2, or substantially similar requests where permissible, must be made readily accessible.

ITS must verify identity proportionately, record the request, acknowledge it, search relevant systems, consult affected business owners, apply PAIA fees or grounds of refusal where applicable, respond within the prescribed period and document the decision. A request to delete does not override a binding legal, regulatory, contractual, evidential or litigation hold. Refusals must explain available remedies.

19. Security compromises

All suspected losses, disclosures, unauthorised access, acquisition, alteration or destruction of personal information must be reported immediately to the Information Officer or Deputy Information Officer. Evidence must be preserved. ITS will promptly contain the event, protect data subjects, investigate scope and cause, assess roles and legal obligations, document decisions, remediate controls and maintain a security-compromise register.

19.1 Notification test and timing

Where there are reasonable grounds to believe personal information has been accessed or acquired by an unauthorised person, ITS as responsible party must notify the Information Regulator and, subject to lawful delay, affected data subjects unless their identities cannot be established. Notification must be made as soon as reasonably possible after discovery, taking into account the legitimate needs of law enforcement and measures reasonably necessary to determine scope and restore system integrity. POPIA does not prescribe a 72-hour deadline or a GDPR “high-risk” threshold.

19.2 Reporting channel

From 1 April 2025, notification to the Information Regulator must be submitted through the Regulator’s eServices Security Compromises Reporting functionality. The Information Officer or registered delegate must submit the required information, retain the portal reference and provide updates when material facts change. Where ITS is an operator, it must notify the responsible party immediately so that the responsible party can meet section 22 obligations.

19.3 Data-subject communication

Communication must be in writing and reach the data subject through an appropriate channel, including mail, email, a prominent website notice, publication in the news media or as directed by the Regulator. It must provide enough information for protective action, including the possible consequences, measures taken or intended, recommendations, the identity of the unauthorised person if known, and Information Officer contact details. The Regulator may direct notification or delay. External communications require Information Officer approval, except where emergency protective action is authorised under the incident plan.

20. Information Officer and Deputy Information Officer

Role	Details
Information Officer	Henry Dul — Registration number: 2024-011380 — henry@its-mail.co.za
Deputy Information Officer	Elizabeth Randles — liz@its-mail.co.za
Telephone	011 675 2092
Physical address	1st Floor, Quadrum 1, Quadrum Office Park, 50 Constantia Boulevard, Constantia Kloof, 1709
Website	www.independenttrusteeservices.co.za

The Deputy Information Officer may perform only duties properly delegated in writing and must be registered before taking up statutory duties. The Information Officer retains accountability and must keep registration and contact details current with the Regulator.

21. Statutory duties and PAIA integration

The Information Officer must ensure that the compliance framework is developed, implemented, monitored and maintained; personal-information impact assessments are performed; the PAIA Manual is developed, maintained

and made available; internal measures and systems support access requests; awareness sessions are conducted; and cooperation is provided to the Information Regulator. PAIA and POPIA requests, complaints and annual reporting obligations must be coordinated and evidenced.

22. Training and awareness

All personnel with access to personal information must complete induction training and annual refresher training. Higher-risk functions must receive role-specific training on health and special information, data-subject requests, secure handling, phishing, operator duties and breach escalation. ITS will conduct periodic awareness activities and simulated or tabletop incident exercises. Completion and remediation must be recorded.

23. Monitoring, assurance and reporting

Compliance monitoring will be risk-based and include processing-register reviews, privacy notices, impact assessments, access reviews, operator contracts, retention and destruction, rights requests, direct marketing, incidents, training and remedial actions. Material risks, overdue actions and breaches must be escalated to the Information Officer and appropriate governing authority. Independent assurance should be considered where risk, scale or prior findings warrant it.

24. Non-compliance and complaints

Non-compliance may result in corrective action, retraining, access restriction, disciplinary action up to dismissal, termination of a supplier or operator, client remediation, regulatory notification or legal proceedings. Concealment, retaliation or deliberate unauthorised processing is serious misconduct. Data subjects may complain to ITS through the Information Officer or to the Information Regulator using the prescribed complaint channel.

25. Review and change management

This policy must be reviewed at least annually and sooner following legislative or regulatory change, material changes to services, systems, operators or information flows, a significant incident, complaint or audit finding, or a change in risk. Changes require formal approval, version control and communication to affected persons.

26. Regulatory references

- Constitution of the Republic of South Africa, 1996 — section 14.
- Protection of Personal Information Act 4 of 2013 and Regulations Relating to the Protection of Personal Information, 2018.
- Promotion of Access to Information Act 2 of 2000 and applicable regulations.
- Information Regulator Guidance Note on Information Officers and Deputy Information Officers.
- Information Regulator Guidance Note on Direct Marketing, dated 3 December 2024.
- Information Regulator security-compromise reporting requirements and eServices process effective 1 April 2025.
- Regulations relating to the Processing of Data Subjects' Health Information by Certain Responsible Parties, 2026.

27. Approval

Approval field	Details
Approved by	Henry Dul
Capacity	Information Officer
Approval date	15/07/2026
Effective date	15/07/2026
Signature	

Next review: within 12 months after approval, unless an earlier review trigger occurs.

Annexure A: Minimum processing register fields

Field	Required record
Activity and owner	Process name, responsible business owner and systems
Data subjects and information	Categories of persons, personal information and special information
Purpose and justification	Specific purpose and section 11 lawful justification
Collection and notification	Sources and applicable section 18 notice
Recipients and operators	Internal recipients, external recipients, operators and contracts
Transfers	Countries, recipients and section 72 justification
Retention	Retention rule, legal basis, trigger and destruction method
Security	Classification, access and key technical or organisational controls
Rights and risk	Request route, impact assessment and residual risk
Review	Last review, changes, evidence and next review

Annexure B: Security-compromise response workflow

1. Report immediately to the Information Officer or Deputy Information Officer; preserve evidence.
2. Contain the event without unnecessarily destroying logs or forensic evidence; protect affected systems and records.
3. Establish whether ITS is responsible party or operator and notify the responsible party immediately where ITS is operator.
4. Determine the information, systems, data subjects, unauthorised persons, time period and likely consequences.
5. Assess whether there are reasonable grounds to believe personal information was accessed or acquired by an unauthorised person.
6. Notify the Information Regulator through eServices and affected data subjects as soon as reasonably possible where section 22 applies.
7. Record decisions, portal references, communications, containment, recovery, root cause and corrective actions.
8. Monitor implementation and close only after accountable approval and verification of remediation.

Annexure C: Minimum privacy-impact assessment triggers

- new systems, cloud services, artificial intelligence or automated decision tools;
- new or materially changed collections, purposes, recipients or data-linking activities;
- large-scale, systematic, special, children's, biometric or health-information processing;
- cross-border hosting, access or support;
- new operators, surveillance, monitoring or high-risk security architecture;
- changes likely to affect data-subject expectations, rights or potential harm; and
- processing potentially requiring prior authorisation by the Information Regulator.