SHILOH CAPITAL

PRIVATE INVESTMENT · STRATEGIC ADVISORY · M&A

GOVERNANCE & COMPLIANCE POLICY DOCUMENTATION

Privacy Policy

Setting out how Shiloh Capital collects, processes, secures, retains, and discloses personal information, and how data subjects may exercise their rights, in compliance with the Protection of Personal Information Act and the Promotion of Access to Information Act of the Republic of South Africa.

DOCUMENT REFERENCE	VERSION	DOCUMENT OWNER	APPROVED BY
SC-POL-PRV-001	1.0 — June 2026	Information Officer & Compliance Function	Founding Directors

REVIEW FREQUENCY	NEXT REVIEW DATE	FSP AUTHORITY	SUPERVISORY REGULATOR
Annual	June 2027	FyreFem Fund Managers — FSP No. 49359	Information Regulator (SA) & FSCA

POPIA 4/2013 | PAIA 2/2000 | FAIS 37/2002 | FICA 38/2001 | ECTA 25/2002 | COMPANIES ACT 71/2008 | CPA 68/2008 | KING V — PRINCIPLE 13 | ISO 27001:2022 | ISO 9001:2015

POLICY CONTENTS

SECTION 01

Purpose, Scope & Definitions

1.1 Purpose

This Privacy Policy ("the Policy" or "SC-POL-PRV-001") sets out how Shiloh Capital (Pty) Limited and its affiliated entities (collectively "Shiloh Capital", "the Firm", "we", "us", or "our") collect, use, process, secure, retain, and disclose the personal information of the persons with whom we interact. The Policy gives effect to the Firm's obligations as a responsible party under the Protection of Personal Information Act, 4 of 2013 ("POPIA") and as a private body under the Promotion of Access to Information Act, 2 of 2000 ("PAIA").

Shiloh Capital is a transaction advisory, capital raising, and mergers and acquisitions firm operating as a Juristic Representative of FyreFem Fund Managers (Pty) Ltd (FSP No. 49359), an authorised financial services provider regulated by the Financial Sector Conduct Authority. As a participant in the financial services sector, the Firm processes personal information in the ordinary course of rendering advisory and intermediary services, and is committed to doing so lawfully, transparently, and in a manner that respects the constitutional right to privacy enshrined in section 14 of the Constitution of the Republic of South Africa.

This Policy is published on the Firm's website for public review and forms part of Shiloh Capital's integrated governance and compliance architecture, read together with the Conflicts of Interest Policy (SC-POL-COI-001), the Risk Management Policy (SC-POL-RMP-001), the PAIA Manual (SC-PAIA-MAN-001), and the ISO 9001:2015 Quality Management System Manual (SC-QMS-MAN-001).

1.2 Scope

This Policy applies to the processing of personal information relating to all categories of data subject with whom the Firm interacts, including:

- Prospective, current, and former clients, investors, and counterparties, and their directors, employees, beneficial owners, and authorised representatives;
- Visitors to the Firm's website and recipients of the Firm's electronic communications;
- Employees, directors, Key Individuals, representatives, job applicants, contractors, and consultants;
- Suppliers, service providers, operators, and professional advisers; and
- Any other natural or juristic person whose personal information the Firm processes in the course of its business.

The Policy applies to personal information processed by any means, whether in electronic, physical, or any other recorded form, and irrespective of where that information is stored.

1.3 Key Definitions

The following defined terms bear the meanings ascribed to them in POPIA and PAIA, and apply throughout this Policy:

TERM	DEFINITION
Personal Information	Information relating to an identifiable, living natural person and, where applicable, an identifiable, existing juristic person — including names, contact details, identity and registration numbers, financial information, biometric data, correspondence, and any opinion or view about the person.
Processing	Any operation concerning personal information, including its collection, receipt, recording, organisation, storage, updating, retrieval, use, dissemination, distribution, merging, restriction, erasure, or destruction.
Data Subject	The natural or juristic person to whom personal information relates.
Responsible Party	The entity that, alone or with others, determines the purpose of and means for processing personal information. Shiloh Capital is the responsible party in respect of the information described in this Policy.
Operator	A person who processes personal information for a responsible party in terms of a written contract, without coming under the direct authority of that responsible party.
Special Personal Information	Personal information concerning a data subject's religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, biometric information, or criminal behaviour, as defined in section 26 of POPIA.
Information Officer	The head of the Firm (or a duly delegated person) responsible for POPIA compliance and the handling of PAIA requests, who is registered with the Information Regulator and supported by appointed Deputy Information Officers.
Information Regulator	The independent body established under section 39 of POPIA, empowered to monitor and enforce compliance with both POPIA and PAIA.
Consent	Any voluntary, specific, and informed expression of will by which a data subject agrees to the processing of personal information relating to them.
De-identify	To delete information that identifies a data subject, or that can be used by a reasonably foreseeable method to identify the data subject, so that the person can no longer be identified.

Where a defined term used in this Policy is not set out above, it bears the meaning given to it in POPIA, PAIA, or the Financial Advisory and Intermediary Services Act, 37 of 2002, as the context requires.

SECTION 02

Legislative & Regulatory Framework

This Policy has been prepared with reference to, and is intended to comply with, the data protection, access to information, and financial services legislation applicable to the Firm in the Republic of South Africa.

FRAMEWORK	RELEVANCE TO THIS POLICY
Protection of Personal Information Act, 4 of 2013 (POPIA)	The primary statute governing the lawful processing of personal information. Establishes the eight conditions for lawful processing, the rights of data subjects, the obligations of responsible parties and operators, and the powers of the Information Regulator. This Policy gives effect to the Firm's obligations under POPIA in full.
Promotion of Access to Information Act, 2 of 2000 (PAIA)	Gives effect to the constitutional right of access to information. Requires the Firm, as a private body, to maintain a PAIA Manual and to process requests for access to records in accordance with the Act. Sections 50 to 53 govern access to records held by private bodies.
Constitution of the Republic of South Africa, 1996	Section 14 guarantees the right to privacy; section 32 guarantees the right of access to information. POPIA and PAIA give effect to these rights, and this Policy is interpreted consistently with them.
FAIS Act, 37 of 2002 & General Code of Conduct	Requires the protection and confidentiality of client information obtained in the rendering of financial services, and the maintenance of records. Personal information collected for advisory and intermediary purposes is processed consistently with the FAIS record-keeping and confidentiality obligations.
FICA, 38 of 2001	The Financial Intelligence Centre Act requires the Firm to collect, verify, and retain client identification and due diligence information for the prevention of money laundering and terrorist financing. Such processing is mandated by law and is a lawful basis for processing under POPIA.
ECTA, 25 of 2002	The Electronic Communications and Transactions Act governs the collection of personal information through electronic means and recognises the validity of electronic records and communications.
Companies Act, 71 of 2008	Requires the Firm to maintain records of its securities, directors, and prescribed officers, and governs the retention of company records — informing the Firm's retention obligations under this Policy.
Consumer Protection Act, 68 of 2008	Regulates direct marketing and the right of consumers to restrict unwanted communications, read together with section 69 of POPIA.
King V & ISO 27001:2022	King V Principle 13 requires the governing body to govern compliance with applicable laws. ISO 27001 informs the information security controls the Firm applies to safeguard personal information.

SECTION 03

Privacy Commitment & the Eight Conditions

PRIVACY COMMITMENT STATEMENT

Shiloh Capital regards the personal information entrusted to it by its clients, investors, employees, and counterparties as a matter of trust. We are committed to protecting the privacy of every data subject, to processing personal information only for lawful and clearly defined purposes, and to maintaining the confidentiality, integrity, and security of that information throughout its lifecycle. We process personal information in accordance with the eight conditions for lawful processing prescribed by POPIA, and we hold ourselves accountable for that processing to our data subjects and to the Information Regulator.

3.1 The Eight Conditions for Lawful Processing

POPIA prescribes eight conditions that a responsible party must satisfy in order to process personal information lawfully. Shiloh Capital embeds each of these conditions in its processing activities, as summarised on the following page.

ACCOUNTABILITY IN PRACTICE

The Firm takes responsibility for the information it holds.

Shiloh Capital has appointed an Information Officer, registered with the Information Regulator, who is accountable for ensuring that the conditions for lawful processing are given effect to throughout the Firm. Compliance with this Policy is monitored by the Compliance Function and reported to the board of directors. Every employee and representative of the Firm is required to comply with this Policy as a condition of their engagement.

3.2 Application of the Eight Conditions

Condition 1

Accountability

The Firm, as responsible party, ensures that the conditions for lawful processing are complied with at the time of determining the purpose and means of processing and throughout the processing itself.

Condition 2

Processing Limitation

Personal information is processed lawfully, minimally, and in a manner that does not unreasonably infringe privacy. Processing is justified by consent, contract, legal obligation, legitimate interest, or another lawful ground.

Condition 3

Purpose Specification

Information is collected for specific, explicitly defined, and lawful purposes related to the Firm's functions, and the data subject is made aware of those purposes at the point of collection.

Condition 4

Further Processing Limitation

Information is not further processed in a manner incompatible with the purpose for which it was originally collected, unless a lawful exception in section 15 of POPIA applies.

Condition 5

Information Quality

The Firm takes reasonable steps to ensure that personal information is complete, accurate, not misleading, and updated where necessary, having regard to the purpose of processing.

Condition 6

Openness

The Firm maintains documentation of its processing operations and notifies data subjects of the collection of their information and the purposes for which it is collected, as reflected in this Policy.

Condition 7

Security Safeguards

The Firm secures the integrity and confidentiality of personal information through appropriate, reasonable technical and organisational measures against loss, damage, unauthorised access, and unlawful processing.

Condition 8

Data Subject Participation

Data subjects may request confirmation of, and access to, the personal information the Firm holds about them, and may request its correction or deletion in accordance with POPIA.

SECTION 04

Information Officer & Privacy Governance

4.1 Appointment of the Information Officer

In accordance with section 56 of POPIA and section 1 of PAIA, the Information Officer of Shiloh Capital is the head of the Firm. The Information Officer is registered with the Information Regulator and is accountable for the Firm's compliance with POPIA and for the handling of requests for access to information under PAIA. The Information Officer is supported by one or more appointed Deputy Information Officers, who assist in the discharge of these duties and to whom requests and queries may be directed in the first instance.

4.2 Responsibilities of the Information Officer

- Encouraging and monitoring the Firm's compliance with the conditions for lawful processing under POPIA;
- Dealing with requests made to the Firm under POPIA and PAIA;
- Working with the Information Regulator in relation to investigations and prior authorisations;
- Ensuring that a compliance framework is developed, implemented, monitored, and maintained;
- Ensuring that a personal information impact assessment is conducted where appropriate;
- Ensuring that this Policy and the PAIA Manual are developed, monitored, maintained, and made available; and
- Ensuring that internal awareness sessions are conducted regarding the Firm's privacy obligations.

4.3 Governance & Oversight

ROLE	PRIVACY RESPONSIBILITY
Board of Directors	Approves this Policy; exercises oversight of the Firm's compliance with applicable privacy and access-to-information legislation consistent with King V Principle 13.
Information Officer (Head of Firm)	Holds ultimate accountability for POPIA and PAIA compliance; registered with the Information Regulator; final authority on access requests.
Deputy Information Officer (Compliance Officer)	Handles day-to-day privacy queries, access requests, and data subject requests; maintains the compliance framework and processing records.
Employees & Representatives	Comply with this Policy; process personal information only as authorised; report suspected security compromises without delay.

SECTION 05

Personal Information We Collect

The categories of personal information the Firm processes depend on the nature of the relationship and the services rendered. We collect only such information as is adequate, relevant, and not excessive for the purposes for which it is processed.

CATEGORY	EXAMPLES OF INFORMATION PROCESSED
Identification Information	Full names, identity or passport numbers, date of birth, nationality, and, for juristic persons, registration numbers and details of directors and beneficial owners.
Contact Information	Postal and physical addresses, email addresses, and telephone numbers.
Financial Information	Banking details, source of funds and wealth, investment objectives, tax information, and creditworthiness, where relevant to the services rendered.
Due Diligence Information	Information collected to satisfy FICA and FAIS obligations, including verification documents, politically exposed person status, and sanctions screening results.
Transactional Information	Records of mandates, instructions, advice given, transactions concluded, and related correspondence.
Employment & Recruitment Information	For employees, applicants, and contractors: curricula vitae, qualifications, references, remuneration, and records required by labour and tax legislation.
Technical & Website Information	Internet protocol addresses, browser type, device information, and information collected through cookies when you visit the Firm's website (see Section 14).
Special Personal Information	Processed only where permitted by law or with consent — for example, criminal-behaviour screening required for regulatory due diligence (see Section 08).

Where the provision of certain personal information is required by law or is necessary to enter into or perform a contract, a failure to provide that information may prevent the Firm from rendering the relevant service.

SECTION 06

How We Collect Personal Information

6.1 Collection Directly from the Data Subject

In accordance with section 11 of POPIA, the Firm collects personal information directly from the data subject wherever practicable — for example, when you complete an onboarding or mandate document, submit an enquiry through the website, enter into an agreement with the Firm, or correspond with us.

6.2 Collection from Other Sources

POPIA permits the collection of personal information from sources other than the data subject in defined circumstances, including where the information is contained in a public record, has deliberately been made public by the data subject, where collection from another source would not prejudice the data subject, or where collection is necessary to comply with a legal obligation. On this basis the Firm may collect information from:

- Public registers and records, including the Companies and Intellectual Property Commission and the deeds registry;
- Credit bureaux, sanctions and politically exposed person databases, and other verification and screening services;
- Your authorised representatives, advisers, employers, or the entities you represent; and
- Counterparties and co-advisers to a transaction in which you are involved.

6.3 Notification at the Point of Collection

When the Firm collects personal information, it takes reasonably practicable steps to ensure that the data subject is aware of the information being collected, the purpose of collection, whether the supply of the information is voluntary or mandatory, the consequences of a failure to provide it, and the existence of the right of access to and correction of the information. Where information is collected indirectly, the data subject is notified unless an exception in section 18(4) of POPIA applies.

6.4 Information Relating to Third Parties

Where a data subject provides the Firm with personal information relating to another person — for example, a beneficial owner, employee, or family member — the data subject warrants that they are authorised to provide that information and that the relevant person has been made aware of this Policy.

SECTION 07

Purpose & Lawful Basis for Processing

The Firm processes personal information only where a lawful basis recognised by section 11 of POPIA applies. The principal purposes for which personal information is processed, and the corresponding lawful basis, are set out below.

PURPOSE OF PROCESSING	LAWFUL BASIS (SECTION 11 POPIA)
Rendering transaction advisory, capital raising, and M&A services to clients and investors	Performance of, or conclusion of, a contract with the data subject; legitimate interests of the Firm and the data subject.
Client onboarding, identity verification, and due diligence	Compliance with a legal obligation under FICA and the FAIS Act.
Anti-money-laundering, sanctions, and regulatory screening	Compliance with a legal obligation.
Communicating with clients, investors, and counterparties	Performance of a contract; legitimate interests; consent where applicable.
Record-keeping, audit, accounting, and tax compliance	Compliance with legal obligations under the FAIS Act, the Companies Act, and the Income Tax Act.
Managing employment, recruitment, and contractor relationships	Performance of a contract; compliance with labour and tax legislation.
Administering, securing, and improving the Firm's website	Legitimate interests of the Firm; consent for non-essential cookies.
Direct marketing of the Firm's services to existing clients	Legitimate interests; consent where required by section 69 of POPIA.
Establishing, exercising, or defending legal claims	Legitimate interests of the Firm; protection of a legitimate interest of the data subject.

Where the Firm relies on consent as the lawful basis for processing, the data subject may withdraw that consent at any time, subject to legal or contractual restrictions and reasonable notice. The withdrawal of consent does not affect the lawfulness of processing carried out before the withdrawal.

SECTION 08

Special & Children's Information

8.1 Special Personal Information

The processing of special personal information is prohibited under section 26 of POPIA unless a general authorisation in section 27 or a specific authorisation in sections 28 to 33 applies. The Firm does not process special personal information except where one of the following grounds is satisfied:

- The data subject has consented to the processing;
- The processing is necessary for the establishment, exercise, or defence of a right or obligation in law;
- The processing is necessary to comply with an obligation of international public law; or
- The information has deliberately been made public by the data subject.

In the financial services context, the Firm may be required to process information concerning criminal behaviour — for example, the results of regulatory and sanctions screening — for the purpose of complying with FICA and the FAIS Act. Such processing is undertaken only to the extent required by law and is subject to the security safeguards in Section 11.

8.2 Personal Information of Children

The processing of the personal information of a child (a natural person under the age of 18 years) is prohibited under section 34 of POPIA unless a ground in section 35 applies, including the prior consent of a competent person such as a parent or guardian. The Firm's services are directed at adults and juristic persons and are not intended for children. The Firm does not knowingly collect the personal information of children except where it is necessary for a lawful purpose — for example, where a child is a beneficiary of a trust or estate — and then only with the consent of a competent person and subject to appropriate safeguards.

8.3 Prior Authorisation

Where the Firm proposes to undertake processing that requires the prior authorisation of the Information Regulator under section 57 of POPIA, it will obtain that authorisation before the relevant processing commences.

SECTION 09

Disclosure, Operators & Third Parties

The Firm treats personal information as confidential and does not sell personal information. We disclose personal information only where it is necessary for a lawful purpose described in this Policy, and subject to appropriate safeguards. Recipients may include:

RECIPIENT	REASON FOR DISCLOSURE
FyreFem Fund Managers	As the licensed financial services provider of which the Firm is a Juristic Representative, for regulatory supervision and compliance oversight.
Operators & Service Providers	Information technology, cloud hosting, document management, verification, and professional support providers who process information on the Firm's behalf under written contracts that require confidentiality and security.
Professional Advisers	Attorneys, auditors, accountants, and tax advisers engaged by the Firm or a transaction, bound by professional duties of confidentiality.
Counterparties & Co-Advisers	Other parties to a transaction in which the data subject is involved, to the extent necessary to advance the mandate.
Regulators & Authorities	The FSCA, the Financial Intelligence Centre, the Information Regulator, the South African Revenue Service, and other authorities, where required by law.
Courts & Legal Process	Where disclosure is required by court order, subpoena, or other legal process, or to establish, exercise, or defend a legal claim.

9.1 Obligations of Operators

Where the Firm engages an operator to process personal information on its behalf, that operator is required, in terms of a written agreement, to process the information only with the knowledge or authorisation of the Firm, to treat it as confidential, and to establish and maintain the security measures required by section 21 of POPIA. Operators are required to notify the Firm immediately where there are reasonable grounds to believe that personal information has been accessed or acquired by an unauthorised person.

SECTION 10

Cross-Border Transfers of Personal Information

The Firm may transfer personal information to a recipient in a foreign country — for example, where a cloud service provider stores information outside the Republic, or where a cross-border transaction requires the disclosure of information to a foreign counterparty or adviser. The Firm transfers personal information across borders only where one of the conditions in section 72 of POPIA is satisfied, namely:

- The recipient is subject to a law, binding corporate rules, or a binding agreement that provides an adequate level of protection substantially similar to that provided by POPIA, including in respect of onward transfers;
- The data subject consents to the transfer;
- The transfer is necessary for the performance of a contract between the data subject and the Firm, or for the implementation of pre-contractual measures taken in response to the data subject's request;
- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the Firm and a third party; or
- The transfer is for the benefit of the data subject, and obtaining consent is not reasonably practicable, but the data subject would be likely to consent if it were.

Where the Firm relies on a binding agreement with a foreign operator, that agreement requires the operator to maintain protections substantially similar to those required by POPIA, and prohibits the onward transfer of personal information except in accordance with equivalent safeguards.

SECTION 11

Security Safeguards & Breach Notification

11.1 Security Measures

In accordance with section 19 of POPIA, the Firm 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. These measures include:

- Access controls, authentication, and the principle of least-privilege access to systems and records;
- Encryption of information in transit and at rest where appropriate, and secure backup arrangements;
- Physical security controls at the Firm's premises and secure storage of physical records;
- Confidentiality undertakings binding all employees, representatives, and operators; and
- Periodic review of security controls, informed by recognised standards including ISO 27001.

The Firm regularly identifies reasonably foreseeable internal and external risks to personal information, establishes and maintains appropriate safeguards against those risks, and verifies that the safeguards are effectively implemented.

11.2 Notification of Security Compromises

Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by an unauthorised person, the Firm will, in accordance with section 22 of POPIA, notify the Information Regulator and the affected data subject as soon as reasonably possible after the discovery of the compromise, unless the identity of the data subject cannot be established. The notification will provide sufficient information to allow the data subject to take protective measures, including a description of the possible consequences, the measures the Firm intends to take, and what the data subject can do to mitigate the adverse effects.

SECTION 12

Retention & Destruction of Records

In accordance with section 14 of POPIA, the Firm does not retain personal information for longer than is necessary to achieve the purpose for which it was collected, unless retention is required or authorised by law, the data subject has consented to longer retention, or the information is required for the establishment, exercise, or defence of a legal claim.

RECORD TYPE	INDICATIVE RETENTION PERIOD
FICA client identification and verification records	At least five years from the termination of the business relationship, as required by FICA.
FAIS client records, advice, and transaction records	At least five years, as required by the FAIS Act and General Code of Conduct.
Accounting, tax, and company records	As required by the Companies Act and the Tax Administration Act (generally five years or longer).
Employment records	As required by applicable labour and tax legislation.
Website and marketing data	Retained only for as long as necessary for the relevant purpose, or until consent is withdrawn.

Upon expiry of the applicable retention period, the Firm destroys, deletes, or de-identifies personal information in a manner that prevents its reconstruction in an intelligible form. The destruction of records is carried out securely, and records of such destruction are maintained where required.

SECTION 13

Your Rights as a Data Subject

POPIA confers a number of rights on data subjects in respect of their personal information. Subject to the conditions and limitations in POPIA, you have the following rights, which you may exercise by contacting the Information Officer:

RIGHT	DESCRIPTION
Right to be Notified	To be notified that your personal information is being collected, and where it has been accessed by an unauthorised person.
Right of Access	To request confirmation of whether the Firm holds your personal information, and to request a record or description of that information, subject to the prescribed fees under PAIA.
Right to Correction & Deletion	To request the correction of inaccurate, irrelevant, excessive, outdated, or incomplete information, or the deletion of information the Firm is no longer authorised to retain.
Right to Object	To object, on reasonable grounds, to the processing of your personal information where processing is based on legitimate interests or the public interest.
Right to Withdraw Consent	To withdraw consent previously given, subject to legal or contractual restrictions and reasonable notice.
Right to Object to Direct Marketing	To object to the processing of your information for purposes of direct marketing, including by unsolicited electronic communication.
Right to Complain	To submit a complaint to the Information Regulator regarding the alleged interference with the protection of your personal information (see Section 17).

A request to exercise a right may be made using the prescribed form and must be directed to the Information Officer at the contact details in Section 17. The Firm will respond to requests within the periods prescribed by POPIA and PAIA. Certain requests may be subject to a prescribed fee, of which you will be notified in advance.

SECTIONS 14 & 15

Cookies, Website Data & Direct Marketing

14.1 Cookies & Website Data

The Firm's website may use cookies and similar technologies to enable the website to function, to remember your preferences, and to understand how the website is used. Cookies are small text files placed on your device when you visit a website.

COOKIE TYPE	PURPOSE
Strictly Necessary	Required for the website to operate; cannot be disabled through the website's controls.
Performance & Analytics	Help the Firm understand how visitors use the website so that it can be improved. Used only with consent.
Functional	Remember your choices and preferences to enhance your experience. Used only with consent.

You may accept or decline non-essential cookies, and you may set your browser to refuse cookies or to alert you when cookies are being used. Declining certain cookies may affect the functionality of the website.

15.1 Direct Marketing

The Firm may send you information about its services where it is lawful to do so. In accordance with section 69 of POPIA, the Firm will not send unsolicited electronic communications for the purpose of direct marketing unless you have consented, or you are an existing client and the marketing relates to similar services, in which case you will be given a reasonable opportunity to object. You may at any time request that the Firm cease sending you direct marketing communications, at no cost and without having to provide a reason, by using the unsubscribe facility in the communication or by contacting the Information Officer.

SECTION 16

Access to Information under PAIA

16.1 The Firm's PAIA Manual

Shiloh Capital is a private body for the purposes of PAIA. In accordance with section 51 of PAIA, the Firm has compiled a PAIA Manual (SC-PAIA-MAN-001) describing the records it holds, the procedure for requesting access, and the contact details of the Information Officer. The PAIA Manual is available, free of charge, on the Firm's website and at its registered offices, and on request from the Information Officer.

16.2 Requesting Access to a Record

A requester who wishes to access a record held by the Firm must complete the prescribed request form (Form 2 — Request for Access to Record of Private Body), submit it to the Information Officer, identify the record sought with sufficient particularity, state the right sought to be exercised or protected, and explain why the requested record is required for the exercise or protection of that right.

16.3 Fees, Grounds for Refusal & Remedies

- **Fees.** A request fee and access fees, as prescribed in the PAIA Regulations, are payable in respect of requests for access. The current prescribed fees are set out in the PAIA Manual.
- **Grounds for refusal.** The Firm may refuse access where a ground for refusal in Chapter 4 of Part 3 of PAIA applies — including the mandatory protection of the privacy of third parties, commercial information, confidential information, and records protected by legal professional privilege.
- **Remedies.** Where a request for access is refused, the requester may apply to a court for appropriate relief under section 78 of PAIA, or lodge a complaint with the Information Regulator, within the periods prescribed by the Act.

The Firm processes PAIA requests within the periods prescribed by the Act and notifies the requester of its decision, the applicable fees, and the available remedies.

SECTION 17

Complaints & the Information Regulator

If you have a query or concern regarding this Policy or the manner in which the Firm processes your personal information, we encourage you to contact the Information Officer in the first instance, so that we may address the matter directly.

SHILOH CAPITAL — INFORMATION OFFICER

Attention: The Information Officer (Office of the Managing Director), supported by the Deputy Information Officer (Compliance Function)
Address: Office 212, Max Office Park, 145 Second Street, Parkmore, Sandton, 2196
Telephone: +27 (0) 10 109 0787
Email: lmukuwane@shilohcap.com
Website: shilohcap.com

If you are not satisfied with the manner in which the Firm has handled your query, or if you believe that the Firm has interfered with the protection of your personal information, you have the right to lodge a complaint with the Information Regulator.

THE INFORMATION REGULATOR (SOUTH AFRICA)

Physical: JD House, 27 Stiemens Street, Braamfontein, Johannesburg, 2001
Postal: P.O. Box 31533, Braamfontein, Johannesburg, 2017
Telephone: 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
Website: inforegulator.org.za

17.1 Amendments to This Policy

The Firm reviews this Policy at least annually and may amend it from time to time to reflect changes in law, regulatory guidance, or its business practices. The current version is published on the Firm's website, and the effective date and version number appear in the document control section. Continued engagement with the Firm following the publication of an amended Policy constitutes acknowledgement of the amended terms.

SECTION 18

Document Control & Founder Approval

18.1 Related Documents

DOCUMENT REF	TITLE & RELATIONSHIP TO THIS POLICY
SC-PAIA-MAN-001	PAIA Manual — records held and the procedure for access requests.
SC-POL-COI-001	Conflicts of Interest Policy — management of conflicts in the handling of information.
SC-POL-RMP-001	Risk Management Policy — information and conduct risk.
SC-QMS-MAN-001	ISO 9001:2015 Quality Manual — records and information controls.

18.2 Document Control

Document Title	Shiloh Capital Privacy Policy
Document Reference	SC-POL-PRV-001
Version	1.0 (June 2026)
Effective Date	1 June 2026
Prepared By	Compliance Function & Office of the Information Officer
Approved By	The Founding Directors of Shiloh Capital (Pty) Ltd
Next Review Date	June 2027 (or earlier upon material legislative change or change in processing practices)
Distribution	Published on the Firm's website for public review; available on request from the Information Officer.