POLARSTAR MANAGEMENT PTY LTD.

PROMOTION TO ACCESS TO INFORMATION - PAIA MANUAL

Prepared in Terms of Section 51 of the Promotion of Access to Information Act 2 of 2000 (as Amended)

July 2023

POLARSTAR

Table of Contents

DOCUMENT CONTROL 3

1. INTRODUCTION 3
2. POLICY STATEMENT 3
3. DEFINITIONS 3
4. POLICY PURPOSE 6
5. DUTIES OF THE INFORMATION OFFICER 7
6. NOTICE 11
7. AVAILABILITY OF THE MANUAL 12
8. POLICY STATEMENT REGARDING REVIEW & UPDATE PROCEDURES 12

ANNEXURE A: POLAR STAR'S CONTACT DETAILS & BUSINESS 13

ANNEXURE B: GUIDE ON HOW TO USE PAIA AND HOW TO OBTAIN ACCESS TO THE GUIDE (SECTION 10 OF THE PAIA GUIDE) 14

ANNEXURE C: STATUTORY RECORDS 15

ANNEXURE D: AVAILABILTY OF RECORDS 16

ANNEXURE E: REQUEST PROCEDURE 17

ANNEXURE F: PRESCRIBED FEES 18

ANNEXURE G: PROCESSING OF PERSONAL INFORMATION 19

ANNEXURE H: DEPUTY INFORMATION OFFICER APPOINTMENT 23

DOCUMENT CONTROL

Version	Date	Change Details:
1.0	February 2022	Creation
2.0	July 2022	General Review
3.0	July 2023	Annual Review

1. INTRODUCTION

PolarStar Management (Pty) Ltd. ("PolarStar" or "Company") is a private body registered financial services provider with FSP No. 45053 that transacts business in the following license categories:

The Company provides advice and intermediary services by making direct or indirect recommendations to clients or by providing research or opinions on financial services and by providing the associated intermediary services and support. The Company is compensated for providing this analysis and advice. The FSP services institutional clients only.

2. POLICY STATEMENT

This Promotion to Access to Information - PAIA Manual ("Policy" or "PAIA Manual") forms part of the internal business processes and procedures of PolarStar Management (Pty) Ltd. ("PolarStar", "Company", "Organisation", "Policy Owner").

The Company's Board of Directors, its employees, consultants, contractors, suppliers and any other persons acting on behalf of the organisation are required to familiarise themselves with the Policy's requirements and undertake to comply with the stated processes and procedures.

Risk owners and control owners are responsible for overseeing and maintaining control procedures and activities.

3. DEFINITIONS

Data Subject

The Person (as defined below) to whom Personal Information (as defined below) relates.

Deputy Information Officer

The deputy information officer of a private body is an employee of that public body or private body to whom the Information Officer has delegated their powers and duties in terms of the Protection of Personal Information Act 4 of 2013 ("POPI" or "POPIA ").

Deputy Information Officer of PolarStar:

Name: Johann Theron

E-mail: johann@polarstarfunds.com

Telephone: +27 21 409 7128

Head

In relation to a private body means:

- in the case of a natural person, that natural person or any person duly authorised by that natural person;
- in the case of a partnership, any partner of the partnership or any person duly authorised by the partnership;
- in the case of a juristic person:
  - the chief executive officer or equivalent officer of the juristic person or any person duly authorised by that officer; or
  - the person who is acting as such or any person duly authorised by such acting person.

Head of PolarStar for the purpose of this Policy:

Name: Herman Verwey

E-mail: herman@polarstarfunds.com

Telephone: + 27 21 409 7109

Information Officer

The Information Officer of PolarStar is designated by the Board of Directors.

Information Officer of PolarStar:

Name: Herman Verwey

E-mail: herman@polarstarfunds.com

Telephone: + 27 21 409 7109

Information Regulator

The Regulator established in terms of Section 39 of POPI.

PAIA

The Promotion of Access to Information Act 2 of 2000.

Person

A natural person or a juristic person.

Personal Information

- Information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to: information relating to the race, gender, sex, pregnancy, marital status, national, ethnic, or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language, and birth of the person;

- Information relating to the education or the medical, financial, criminal or employment history of the person;
- Any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person, the biometric information of the person;
- The personal opinions, views, or preferences of the person; correspondence sent by the person 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 the person; and the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

Personal Requester

A requester seeking access to a record containing personal information about the requester.

POPI

The Promotion of Personal Information Act 4 of 2013.

Private body

- a natural person who carries or has carried on any trade, business, or profession, but only in such capacity
- a partnership which carries or has carried on any trade, business, or profession; or
- any former or existing juristic person, but excludes a public body.

Processing

Any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use, dissemination by means of transmission, distribution or making available in any other form, or merging, linking, as well as restriction, degradation, erasure, or destruction of information.

Requester

In relation to a private body, means any person, including, but not limited to public body or an official thereof, making a request for access to a record of the organisation or a person acting on behalf of such person.

Request for access

A request for access to a record of the organisation in terms of Section 50 of PAIA.

Record

Any recorded information regardless of the form or medium, in the possession or under the control of the organisation irrespective of whether or not it was created by the organisation.

Third Party

In relation to a request for access to a record held by the organisation, means any person other than the requester.

4. POLICY PURPOSE

The Promotion of Access to Information Act, 2000 gives effect to section 32 of the Constitution, which provides that everyone has the right to access information held by the State or any other person (or private body), when that information is required for the exercise or protection of any rights.

The purpose of PAIA is to:

- foster a culture of transparency and accountability in public and private bodies by giving effect to the right of access to information, and to
- actively promote a society in which the people of South Africa have effective access to information to enable them to exercise and protect all of their rights more fully.

The organisation recognises everyone's right to access to information and is committed to provide access to the organisation's records where the proper procedural requirements as set out by PAIA and POPI have been met.

The organisation's PAIA manual is compiled in accordance with section 51 of the Act and contains the following provisions:

Annexure A: PolarStar's Contact Details & Business Type
This section provides the organisations postal and street address, phone, and fax number and the e-mail address of the head of the organisation.

Annexure B: Guide on How to Use PAIA and How to Obtain Access to The Guide (Section 10 PAIA Guide)
This section provides a description of the guide referred to in Section 10 of PAIA and how you may obtain access to it.

Annexure C: Statutory Records
This section provides a description of the various statutes in terms of which the organisation is required to maintain records.

Annexure D: Availability of Records
This section provides a list of records of the Company which are available without a person having to request access.

Annexure E: Request Procedure
This section sets out the procedure required to obtain access to a record indicated as a "PAIA Request".

Annexure F: Prescribed Fees
This section sets out the fees that are payable to the organisation prior to processing a request to obtain access to a record held by the organisation.

Annexure G: Processing of Personal Information
This section sets out the applicable aspects for the processing of personal information.

Annexure H: Deputy Information Officer Appointment
This section provides for the formal appointment of a Deputy Information Officer where so required.

5. DUTIES OF THE INFORMATION OFFICER

The Information Officer and/or the Deputy Information Officer of the organisation are responsible for:

- Publishing and proper communication of the manual i.e., creating policy awareness;
- Facilitating any request for access;
- Providing adequate notice and feedback to the requester;
- Determining whether to grant a request for access to a complete/full record or only part of a record;
- Ensuring that access to a record, where so granted, is provided timeously and in the correct format;
- Reviewing the policy for accuracy and communicating any amendments.

Right of Access

The Information Officer (Herman Verwey) may only provide access to any record held by the organisation to a requester if:

- The record is required for the exercise or protection of any right;
- The requester complies with the procedural requirements relating to a request for access to that record; and
- The access to that record is not refused in terms of any of the grounds for refusal listed below.

Grounds for Refusal

The Information Officer Herman Verwey must assess whether there are any grounds for refusing a request for access.

Where any grounds for refusal are found, a request for access will not be granted.

However, despite finding any grounds for refusal, access to the record(s) will be provided where:

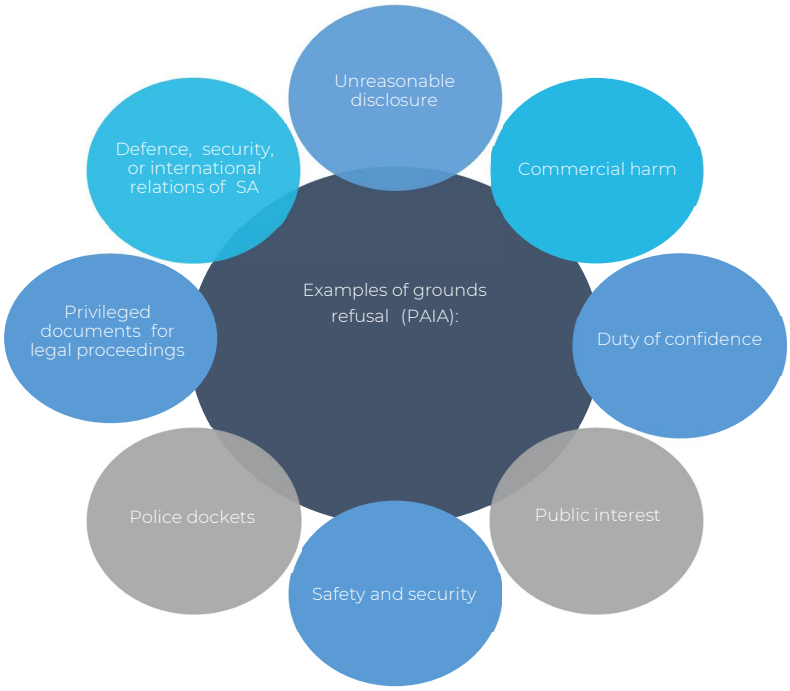
- the disclosure of the record would reveal evidence of a substantial contravention of, or failure to comply with the law or imminent and serious public or environmental risk, and
- the public interest in disclosing record, will clearly outweigh the harm contemplated in the provision in question.

Where there are no grounds for refusal, request for access will be granted.

If a request for access is made with regards to a record containing information that would justify a ground for refusal, every part of the record which

- does not contain, and
- can reasonably be severed from any part that contains, any such information must, despite any other provision of PAIA, also be disclosed.

The grounds for refusal, or absence thereof, are set out below:



A: Mandatory Protection of privacy of a Third Party who is a Natural Person

Grounds for Refusal:

The disclosure would involve the unreasonable disclosure of personal information about a third party that is a natural person (including a deceased individual)

No Grounds for Refusal:

- The record consists of information that concerns an individual who has already consented in writing to its disclosure to the requester concerned;
- The record consists of information that is already publicly available;
- The record consists of information that was given to the organisation by the individual to whom it relates, and the individual was informed by or on behalf of the organisation, before it is given, that the information belongs to a class of information that would or might be made available to the public;
- The record consists of information about an individual's physical or mental health, or well-being, who is under the care of the requester and who is under the age of 18; or incapable of understanding the nature of the request, and if giving access would be in the individual's best interest;
- The record consists of information about an individual who is deceased, and the requester is the individual's next of kin or making the with the written consent of the individual's next of kin;
- The record consists of information about an individual who is or was an official of the organisation and which relates to the position or functions of the individual, including, but not limited to the title, work address, work phone number, the classification, salary scale or remuneration and responsibilities of the position heled, or services performed by the individual;
- the name of the individual on a record prepared by the individual in the course of employment.

B: Mandatory Protection of Commercial Information of a Third Party

Grounds for Refusal

- The record consists of information that contains trade secrets of a third party;
- The record consists of information that contains financial, commercial, scientific, or technical information, other than trade secrets, of a third party, the disclosure of which would be likely to cause harm to the commercial or financial interests of that third party;
- The record consists of information supplied in confidence by a third party, the disclosure of which could reasonably be expected to put that third party at a disadvantage in contractual or other negotiations or to prejudice that third party in commercial competition.

No Grounds for Refusal

The Information Officer Herman Verwey must assess whether there are any grounds for refusing a request for access.

Where any grounds for refusal are found, a request for access will not be granted.

However, despite finding any grounds for refusal, access to the record(s) will be provided where:

- the disclosure of the record would reveal evidence of a substantial contravention of, or failure to comply with the law or imminent and serious public or environmental risk, and
- the public interest in disclosing record, will clearly outweigh the harm contemplated in the provision in question.

Where there are no grounds for refusal, request for access will be granted.

If a request for access is made with regards to a record containing information that would justify a ground for refusal, every part of the record which

- does not contain, and
- can reasonably be severed from any part that contains, any such information must, despite any other provision of PAIA, also be disclosed.

The grounds for refusal, or absence thereof, are set out below:

- The record consists of information about a third party who has already consented in writing to its disclosure to the requester concerned

The record consists of information about the results of any product or environmental testing or other investigation supplied by a third party or the results of any such testing or investigation carried out by or on behalf of a third party and its disclosure would reveal a serious public safety or environmental risk (the results of any product or environmental testing or other investigation do not include the results of preliminary testing or other investigation conducted for the purpose of developing methods of testing or other investigation.

C: Mandatory Protection of certain Confidential Information of a Third Party

Grounds for Refusal

- The record consists of the disclosure of information of which would constitute an action for breach of a duty of confidence owed to a third party in terms of an agreement

D: Mandatory Protection of Safety of Individuals and Protection of Property

Grounds for Refusal

- The record consists of information that if disclosed could reasonably be expected to endanger the life or physical safety of an individual
- The record consists of information that if disclosed would likely prejudice or impair the security of a building, a structure or system, a computer or communication system, a means of transport, any other property
- The record consists of information that if disclosed would likely prejudice or impair the security of methods, systems, plans or procedures for the protection of an individual in accordance with a witness protection scheme, the safety of the public, or any part of the public, or the security of property

E: Mandatory Protection of Records privileged from Production in Legal Proceedings

Grounds for Refusal

The record consists of information privileged from production in legal proceedings unless the person entitled to the privilege has waived the privilege

F: Commercial Information of the Organisation

Grounds for Refusal

The record consists of information that contains trade secrets of the organisation

- The record consists of information that contains financial, commercial, scientific, or technical information, other than trade secrets, of the organisation, the disclosure of which would likely cause harm to the commercial or financial interests of the organisation
- The record consists of information, the disclosure of which, could reasonably be expected to put the organisation at a disadvantage in contractual or other negotiations or prejudice the organisation in commercial competition
- The record is a computer program as defined in section 1(1) of the Copyright Act (Act 98 of 1978), owned by the organisation, except insofar as it is required to give access to a record to which access is granted in terms of PAIA

No Grounds for Refusal

The record consists of information about the results of any product or environmental testing or other investigation supplied by the organisation or the results of any such testing or investigation carried out by or on behalf of the organisation and its disclosure would reveal a serious public safety or environmental risk (the results of any product or environmental testing or other investigation do not include the results of preliminary testing or other investigation conducted for the purpose of developing methods of testing or other investigation)

G: Mandatory Protection of Research Information of a Third Party and the Organisation

Grounds for Refusal

- The record consists of information that contains information about research being or to be carried out by or on behalf of a third party, the disclosure of which would be likely to expose the third party, a person that is or will be carrying out the research on behalf of the third party, or the subject matter of the research to serious disadvantage
- The record consists of information that contains information about research being or to be carried out by or on behalf of the organisation, the disclosure of which would be likely to expose the organisation, a person that is or will be carrying out the research on behalf of the organisation, or the subject matter of the research to serious disadvantage

6. NOTICE

Where a request for access has been received, the Information Officer (Herman Verwey) will notify the requester of receipt and the prescribed fee (if any) that is payable prior to processing the request. Please refer to Annexure F for a full breakdown of fees payable. Personal requesters will not be charged a request fee.

The notice must state:

- The amount of the deposit payable (if any);
- That the requester may lodge a complaint with the Information Regulator or an application with a court against the tender or payment of the request fee, or the tender or payment of a deposit, as the case may be;
- The procedure (including the period) for lodging the complaint with the Information Regulator or the application.

Except to the extent that the provisions regarding third party notification may apply, the Information Officer and/or Deputy Information Officer to whom the request is made, must as soon as reasonably possible, but in any event within 30 days, after the request has been received in the prescribed format:

- Decide in accordance with PAIA whether to grant the request, and
- Notify the requester of the decision and, if the requester stated that he or she wishes to be informed of the decision in any other manner, inform him or her in that manner, if it is reasonably possible.

If the request for access is granted, the notice must state:

- The access fee (if any) to be paid upon access;
- The form in which access will be given, and
- That the requester may lodge a complaint with the Information Regulator or an application with a court against the access fee to be paid or the form of access granted, and the procedure, including the period allowed, for lodging a complaint with the Information Regulator or the application.

If the request for access is refused, the notice must:

- State adequate reasons for the refusal, including the relevant provision of PAIA that was relied on;
- Exclude, from any such reasons, any reference to the content of the records'; and
- State that the requester may lodge a complaint with the Information Regulator or an application with a court against the refusal of the request, and the procedure (including the period) for lodging a complaint with the Information Regulator or the application.

Should all reasonable steps have been taken to find a record requested, and there are reasonable grounds for believing that the record:

- Is in the organisation's possession, but cannot be found, or
- Simply does not exist, the head of the organisation must, by way of affidavit or affirmation, notify the requester that it is not possible to provide access to that record. The affidavit or affirmation must provide full account of all steps taken to find the record in question or to determine whether the record exists, as the case may be, including all communication with every person who conducted the search on behalf of the head.

7. AVAILABILITY OF THE MANUAL

A hard copy of the Manual is available at the Company's reception at 185 Bree Street, Cape Town -

- to any person upon request and upon the payment of a reasonable prescribed fee; and
- to the Information Regulator upon request.

A fee for a copy of the Manual, as contemplated in annexure B of the Regulations, shall be payable per each A4-size photocopy made.

8. POLICY STATEMENT REGARDING REVIEW & UPDATE PROCEDURES

Aside from at least an annual review of the Policy, there will be times when the Privacy Policy needs to be updated to ensure that it remains in line with the way PolarStar operates and complies with all current laws and legislation. Other events that may result in a policy change may include changes to the IT environment, legislations, processes, procedures, and technologies. PolarStar will inform all employees when material changes to the Policy are made. Material changes include changes to the type of data PolarStar collects or the way we process data.

ANNEXURE A: POLAR STAR'S CONTACT DETAILS & BUSINESS

A. Organisation Contact Details

Postal address: 185 Bree Street, Cape Town
Street address: 185 Bree Street, Cape Town
Phone number: + 27 21 409 7120

B. Information Officer

Full names & surname: Herman Verwey
Email address: info@polarstarfunds.com

C. Business Type

Polar Star FSP Number 45053 is an Authorised Financial Services Provider as defined by the FAIS ACT

ANNEXURE B: GUIDE ON HOW TO USE PAIA AND HOW TO OBTAIN ACCESS TO THE GUIDE (SECTION 10 OF THE PAIA GUIDE)

The South African Human Rights Commission has compiled a guide on how to use PAIA ("Guide").The Regulator has, in terms of section 10(1) of PAIA, as amended, updated, and made available the revised Guide on how to use PAIA ("Guide"), in an easily comprehensible form and manner, as may reasonably be required by a person who wishes to exercise any right contemplated in PAIA and POPIA.

The Guide is available in each of the official languages and in braille.

The aforesaid Guide contains the description of-

- the objects of PAIA and POPIA;
- the postal and street address, phone, and fax number and, if available, electronic mail address of-
    - the Information Officer of every public body,
    - every Deputy Information Officer of every public and private company designated in terms of section 17(1) of PAIA and section 56 of POPIA ;
- the manner and form of a request for
    - access to a record of a public body contemplated in section 11; and
    - access to a record of a private body contemplated in section 50.
- the assistance available from the Information Officer of a public body in terms of PAIA and POPIA;
- the assistance available from the Regulator in terms of PAIA and POPIA;
- all remedies in law available regarding an act or failure to act in respect of a right or duty conferred or imposed by PAIA and POPIA, including the manner of lodging
    - an internal appeal;
    - a complaint to the Regulator; and
    - an application with a court against a decision by the information officer of a public body, a decision on internal appeal or a decision by the Regulator or a decision of the head of a private body.
- the provisions of sections 14 and 51 requiring a public body and private body, respectively, to compile a manual, and how to obtain access to a manual;
- the provisions of sections 15 and 52 providing for the voluntary disclosure of categories of records by a public body and private body, respectively;
- the notices issued in terms of sections 22 and 54 regarding fees to be paid in relation to requests for access; and
- the regulations made in terms of section 92.

Members of the public can inspect or make copies of the Guide from the offices of the public and private bodies, including the office of the Regulator, during normal working hours.

The Guide can also be obtained:

- upon request to the Information Officer.
- from the website of the Regulator (https://inforegulator.org.za/).

PAIA grants a requester access to records of a private body, if the record is required for the exercise or protection of any rights.

Where a public body lodges a request, the public body must be acting in the public interest.

Requests in terms of PAIA shall be made in accordance with the prescribed procedures at the rates provided.

ANNEXURE C: STATUTORY RECORDS

Polar Star (Pty) Ltd maintains statutory records and information in terms of the following legislation:

- Administration of Estates Act 66 of 1965 - Basic Conditions of Employment Act 75 of 1997;
- Companies Act 71 of 2008;
- Compensation of Occupational Injuries and Diseases Act 130 of 1993;
- Competition Act 89 of 1998;
- Electronic Communications and Transaction Act 25 of 2002;
- Employment Equity Act 55 of 1998;
- Financial Advisory and Intermediary Services Act 37 of 2002;
- Financial Intelligence Centre Act 38 of 2001;
- Income Tax Act 58 of 1991;
- Inspection of Financial Institutions Act 80 of 1998;
- Insurance Act 18 of 2017;
- Labour Relations Act 66 of 1995;
- Long-term Insurance Act 52 of 1998;
- Policyholder Protection Rules;
- Prevention of Organised Crime Act 121 of 1998;
- Protection of Constitutional Democracy against Terrorist and Related Activities Act 33 of 2004;
- Protection of Personal Information Act 4 of 2013;
- Short-term Insurance Act 53 of 1998;
- Skills Development Levies Act 9 of 1999;
- Unemployment Insurance Act 30 of 1996;
- Value-added Tax Act 89 of 1991.

ANNEXURE D: AVAILABILTY OF RECORDS

Records of the Company which are available without a person having to request access

The records of the Company which are available without a person having to request access include:

- Annual Financial Reports of the Funds;
- Advertising pamphlets and brochures;
- Newsletters;
- Statutory Notices;
- FAIS Licence Information;
- Conflict of Interest Policy;
- Access to Information Manual;
- Complaints Resolution Policy; and

ANNEXURE E: REQUEST PROCEDURE

Information Requests

In terms of Chapter 1 of Part 3, Section 50 of PAIA, any person may request access to information from the Company, and must be given access to same, provided that:

- The record is required for the exercise or protection of any rights;
- The requester complies with the procedural requirements as defined in PAIA for a request to access a record; and
- Access to a record is not refused on any ground for refusal as contemplated in Chapter 4 of Part 3 of PAIA.

In terms of Section 23 of the POPIA, a Data Subject, having provided adequate proof of identity, has the right to:

- Request to confirm, free of charge, whether or not the Company holds personal information about the Data Subject;
- Request the record, or a description of the personal information, held by the Company, including information about the identity of all third parties, or categories of third parties, who have, or have had access to the information –
    - within a reasonable time;
    - at a prescribed fee, if any;
    - in a reasonable manner and format; and
    - in a form that is generally understandable.

Procedures

Complete the relevant form that can be acquired from the revised Guide referred to in paragraph Annexure B above.

If a request is made on behalf of another person, then the requester must submit proof of the capacity in which the requester is making the request to the reasonable satisfaction of the Information Officer.

Submit the form to the Information Officer at the physical address or electronic mail address, as stated in Annexure A above.

The requester must pay the prescribed fee (as explained in Annexure F below) before any further processing can take place.

The Company will process the request within 30 days, unless the requestor has stated special reasons, which would satisfy the Information Officer that circumstances dictate that the above time periods will not be complied with.

Records held by the Company may be accessed by requesters only once the pre-requisite requirements for access have been met. A requester is any person making a request for access to a record of the institution. There are two types of requesters:

- Personal Requester: being a person seeking access to a record containing personal information about him/her/itself; and
- Other Requester: This person is entitled to request access to information on third parties. However, the Company is not obliged to voluntarily grant access.

ANNEXURE F: PRESCRIBED FEES

PAIA provides for two types of fees which can be established by reference to the Guide referred to above:

- A request fee, which will be a standard fee; and
- An access fee, which must be calculated by taking into account reproduction costs, search and preparation time and cost, as well as postal costs.

When the Information Officer receives the request, he/she shall notify the requester to pay the prescribed request fee (if any), before any further processing of the request. The Information Officer may withhold a record until the requester has paid the fees. If a deposit has been paid in respect of a request for access, which is refused, then the Information Officer concerned must repay the deposit to the requester.

The prescribed fees can be found in the Guide referred to in Annexure B above.

ANNEXURE G: PROCESSING OF PERSONAL INFORMATION

1. Purpose of Processing Personal Information

To render financial service, tour our clients as proscribed by the FAIS Act.

2. Description of the categories of Data Subjects and of the information or categories of information relating thereto

Categories of Data Subjects	Personal Information that may be processed
Customers / Clients	Name, Last name, Identity number, Passport number, Date of birth (not age), Age (not date of birth), Gender, Nationality, Photographs, residential address, First name of children under 18 years of age, Last name of children under 18 years of age, Birth information of children under 18 years of age, Identity number of children under 18 years of age, E-mail address, Home postal address, Home telephone number, Personal cellular, mobile or wireless number, Business e-mail address, Business postal address, Business telephone number, Business cellular, mobile or wireless number, Financial institution account number, Tax number
Service Providers	names, registration number, vat numbers, address, and bank details
Employees	address, qualifications, gender, banking details, ID number, Name, Surname, contact number, email address, previous employment, Tax Number, drivers' licence.

3. The recipients or categories of recipients to whom the personal information may be supplied

Specify the person or category of persons to whom the body may disseminate personal information. Below is an example of the category of personal information which may be disseminated and the recipient or category of recipients of the personal information.

Category of personal information	Recipients or Categories of Recipients to whom the personal information may be supplied
Identity number and names, for criminal checks	South African Police Services
Category of personal information	
Qualifications, for qualification verifications	South African Qualifications Authority
Credit and payment history, for credit information	Credit Bureaus
Identity number and names, for criminal checks	Financial Intelligence Centre

4. Planned transborder flows of personal information

The transfer of personal information from the Republic to foreign countries is prohibited unless:

- the person receiving the information is subject to a law, binding corporate rules and/or binding agreement that provides an adequate level of protection that effectively upholds principles for reasonable processing of the information that are substantially similar to the conditions for the lawful processing of personal information relating to a Data Subject who is a natural person and, where applicable, a juristic person and includes provisions, that are substantially similar to the provisions of POPIA, relating to the further transfer of personal information from the recipient to third parties who are in a foreign country;
- the Data Subject has agreed to the transfer of information;
- such transfer is necessary for the performance of a contract between the Data Subject and the responsible party, or for the implementation of pre-contractual measures taken in response to the Data Subject's request;
- such transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the responsible party and a third party; or
- transfer is for the benefit of the Data Subject and it is not reasonably practicable to obtain their consent and that such consent, if it were reasonably practicable to obtain same, would be likely to have been given.

No processing of data outside of standard operational requirements will be done in regions that are not POPIA, or GDPR. All data processing falls within the South African, or Western European. Any data sharing agreements are explicit and are transparent. No other sharing or processing of data will be performed outside of standard operational or existing data sharing agreements in place with service providers.

5. General description of Information Security Measures to be implemented by the responsible party to ensure the confidentiality, integrity, and availability of the information

Cybersecurity Resilience, IT Infrastructure & Posture

PolarStar believes that the key for minimising the occurrence of an attack to its IT and IS Infrastructure and Cybersecurity is the combination of (i) Responsibility Assignment, (ii) Software and Service Providers, (iii) Assessments; and (iv) Training and Tests.

Responsibility Assignment: From an internal standpoint, PolarStar assigns Cybersecurity responsibilities to its employees to ensure that it has proper governance over its Cybersecurity program. Software and Service Providers: PolarStar ensures that its service providers, including Microsoft 365, Box, Dynamo Software, and Cyberlogic Stellenbosch (Pty) Ltd ("Cyberlogic"), follow Cybersecurity Best Practices. At a minimum, PolarStar ensures that its third-party service providers undergo regular risk assessments, vulnerability assessments, and penetration testing, enforce encryption of data and at rest, and support strong authentication mechanisms, such as multi-factor authentication. For example, Microsoft 365 and Box enforce encryption and offer multi-factor authentication settings. PolarStar also regularly requests confirmation of regular penetration testing if the results are not already publicly available. PolarStar also considers outsourcing risks in its overall risk assessments and risk register. PolarStar ensures an adequate level of oversight and accountability for outsourced functions by maintaining administrative access to endpoints and to Microsoft 365, by receiving regular reports from the third-party service provider CyberLogic, and by performing yearly independent technical assessments of its configuration settings. PolarStar ensures that its cloud computing service providers are industry leaders and can properly handle multi-tenancy and isolation of PolarStar's data. For example, Microsoft 365 and Box possess many regulatory certifications and continually undergo security assessments and penetration testing that verify isolation of customer data. Dynamo Software falls into a similar category, and PolarStar has confirmed that it maintains SOC 2 certification. PolarStar ensures that its cloud computing service providers can properly maintain their stated service level agreements. For example, Microsoft 365 and Box possess many regulatory certifications that require availability guarantees and BCDR testing. Microsoft 365 and Box each maintain 99.9% uptime guarantees. PolarStar ensures that its cloud computing service providers have data removal procedures in place after termination of existing contracts. For example, Microsoft 365 automatically removes customer data 90 days after account termination. PolarStar additionally performs offline backups of files stored in Box to ensure data retention via both hard drive & Google Cloud.

PolarStar is also able to pull logs or run reports from Microsoft 365 audit logs whenever it needs to calculate metrics related to security events. PolarStar follows best practices from a cybersecurity standpoint to ensure protection of data. While PolarStar does use cloud computing services for email and file storage, Microsoft 365 and Box are industry leaders that provide several types of security assurances that PolarStar would not be able to achieve on its own without substantial cost. For example, leveraging Microsoft 365 enables

PolarStar to ensure that its email services are continually kept up to date, made highly available, backed up, and monitored for cyberattacks by industry leading professionals. PolarStar configures these services as securely as possible, such as enabling security defaults for Microsoft 365 to ensure that strong encryption and authentication protocols are required. PolarStar additionally implements Endpoint Detection and Response (EDR) from Sentinel One. EDR is a cybersecurity approach that focuses on detecting and investigating security incidents on endpoints like desktops, laptops, servers, and mobile devices. EDR solutions collect and analyse endpoint data, network traffic, and user behaviour to detect anomalous activities that could indicate a security breach. EDR solutions are designed to provide real-time threat intelligence, automated incident response, and forensic investigation capabilities. EDR tools allow security teams to detect and respond to advanced threats quickly and efficiently, minimizing the risk of data breaches and other cybersecurity incidents. PolarStar enables BitLocker encryption for data at rest for all of its endpoints, and uses updated modern browsers that require HTTPS for data in transit. PolarStar is also able to pull logs or run reports from Microsoft 365 audit logs whenever it needs to calculate metrics related to security events.

Assessments: PolarStar also relies on its cybersecurity partners to perform yearly independent cybersecurity assessments with items derived both from well recognised frameworks and from their own knowledge and experience in the cybersecurity industry to ensure a robust assessment framework.

Training and Tests: PolarStar ensures periodic training and phishing testing for all users provided by external parties. Penetration testing and vulnerability assessments are also conducted at least on an annual basis. Regular training and simulated attacks can stop many attacks and help identify people who are especially vulnerable. The best simulations mimic real-world attack techniques. Simultaneously, PolarStar assumes that users will eventually click some threats. Attackers will always find new ways to exploit human nature. PolarStar implements solutions that spot and block inbound email threats targeting employees before they reach the inbox.

ANNEXURE H: DEPUTY INFORMATION OFFICER APPOINTMENT

In terms of the Protection of Personal Information Act the head of a private body is the designated Information Officer for that private body. The Information Officer may delegate any power or duty conferred or imposed in terms of POPI to the Deputy Information Officer.

The organisation has appointed a Deputy Information Officer to facilitate any requests to access records held by the organisation. This delegation does not prohibit the person who made the delegation from exercising power concerned or performing the duty concerned himself or herself. The delegation may at any time be withdrawn or amended in writing by the person who made the delegation.

The Deputy Information Officer need not have any specific qualifications but must have a thorough knowledge of the organisation's functional departments and business processes.

The Deputy Information Officer has the authority to approach all staff members of the organisation and to request all records held by the organisation. Where a manager is of the opinion that access to a record should not be granted to the Deputy Information Officer, reasons for this decision shall be given to the Information Officer who will make a final decision on the matter.

Together with the Information Officer, the Deputy Information Officer is responsible for:

- Publishing and proper communication of the manual i.e., creating policy awareness
- The facilitation of any request for access
- Providing adequate notice and feedback to the requester
- Determining whether to grant a request for access to a complete/full record or only part of a record
- Ensuring that access to a record, where so granted, is provided timeously and in the correct format
- Reviewing the policy for accuracy and communicating any amendments

The Head of the organisation designated Johann Theron as the Organisation's Deputy Information Officer