PRIVACY AND PROTECTION OF PERSONAL INFORMATION POLICY

DISCLAIMER

This document has been prepared by TriAlpha Investment Management Proprietary Limited, a licensed financial services provider (License Number 28090).

TABLE OF CONTENTS

VERSION HISTORY

Version	Responsible Party	Summary of Changes	Date approved by the Board
V1.0	Simphiwe Khumalo	Creation	17 March 2021
V2.0	Simphiwe Khumalo	Updated Annexure B and Annexure C	20 April 2021
V3.0	Simphiwe Khumalo	Information Regulator's contact details – Updated the office address and removed the old fax and telephone numbers on Annexure E: Manual to Accessing Information.	

1. PURPOSE AND APPLICATION

The Privacy and Protection of Personal Information Policy provides guidelines on how Personal Information is processed and safeguarded by TriAlpha Investment Management Proprietary Limited ("TriAlpha", "we", or "us"), in order to ensure compliance with the Protection of Personal Information Act, 4 of 2013 ("POPIA" or "POPI Act"), which regulates and controls the processing of Personal Information.

This policy without exception will apply to:

- TriAlpha and its subsidiary companies, including all employees thereof, including permanent employees, fixed term contractors, and non-executive directors;
- Any entity or person who processes Personal Information on behalf of TriAlpha, whether residing or operating in South Africa, or overseas.

The POPI Act provides for 8 conditions under which Personal Information may be legally gathered and processed, namely:

- Accountability: ensuring on a consistent basis all conditions and measures set out in the Act are complied with at the time Personal Information is processed. TriAlpha aims to achieve this by developing and maintaining adequate policy and procedure manuals under the tutelage of the Information Officer, our Risk & Compliance Committee and board of directors.
- Processing Limitation: Personal Information may only be processed in a fair and lawful manner and only with the consent of the Data Subject. This policy aims to provide guidance as to how TriAlpha manages the processing of Personal Information to ensure compliance with the Act.
- Purpose Specific: Personal Information may only be processed for specific, explicitly defined and legitimate reasons. This policy and its annexures necessitate continuous monitoring of the use of Personal Information to ensure information is only used for the specific purpose which it was gathered. This is achieved by ensuring regular reviews are conducted to take stock of Personal Information held and ensuring Personal Information is destroyed in a manner that prevents its reconstruction, after authorization is lost to retain such records.
- Further Processing Limitation: Personal Information may not be processed for a secondary purpose unless that processing is compatible with the original purpose. Employee training sessions are catered for in this policy. This is to ensure that all employees are aware that confirmation is required from Data Subjects before Personal Information is used for another purpose other than what the Personal Information was initially gathered for.
- Information Quality: The Responsible Party must take reasonable steps to ensure that Personal Information collected is complete, accurate, not misleading and updated where necessary. This policy sets out processes to ensure that Personal Information held is reliable and accurate at all times. The policy also caters for processes to allow Data Subjects to update their information or withdraw consent.

- Openness: The Data Subject whose information we collect must be aware that we are collecting such Personal Information and understand the purpose the information will be used. This policy sets out the types of Personal Information gathered and processed by the different business divisions and imposes on these divisions the requirements: to assess the basis of processing, to inform the Data Subjects as to why information is being gathered, to inform the Data Subjects of his/her rights to access his/her information and to object to the processing of said information.
- Security Safeguards: Personal Information must be kept secure against risk of loss, unlawful access, interference, modification, unauthorized destruction and disclosure. This policy sets out procedures which aim to identify internal and external risks to Personal Information (Safety and Security Risk Assessment). In addition, appropriate safeguards are put in place to guard against identified risks. These safeguards are reviewed regularly to ensure security protocols are adequately maintained.
- Data Subject Participation: Data Subjects may request confirmation as to whether personal information is held, as well as request the correction and/or deletion of any personal information held about them. This policy sets out the processes followed to allow Data Subjects to correct, delete or amend Personal Information held by us.

2. DEFINITIONS

In order to understand the implications of this document and the objectives of POPIA the following definitions should be noted:

"Biometrics" means a technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition.

"Child" means a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him- or herself.

"Competent Person" means any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child.

"Consent" means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of Personal Information.

"Data Subject" means the person who will provide TriAlpha or its Operator(s) with Personal Information and who consents when providing such Personal Information by way of agreeing to a Privacy and Consent Notice.

"Further Processing Limitation" this is where personal information is received from a third party and passed on to the responsible party for further processing. In these circumstances, the further processing must be compatible with the purpose for which it was initially collected.

"Information Officer" is responsible for ensuring that the organisation complies with Promotion of Access to Information Act ("PAIA") and with the POPI Act. This is a key person in any PAIA or POPIA project.

"Operator" means a natural person or a juristic person who processes a Data Subject's Personal Information on behalf of TriAlpha in terms of a contract or mandate, without coming under the direct authority of TriAlpha.

"Person" means a natural person or a juristic person.

"Personal Information" means information relating to any identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, namely the Data Subject, including, but not limited to—

a) 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;
b) Information relating to the education or the medical, financial, criminal or employment history of the person;
c) Any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
d) The biometric information of the person;
e) The personal opinions, views or preferences of the person;
f) 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;
g) The views or opinions of another individual about the person; and
h) 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.

"Processing" means any operation or activity or any set of operations, whether or not by automatic means, concerning Personal Information, including—

a) The collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
b) Dissemination by means of transmission, distribution or making available in any other form; or
c) Merging, linking, as well as restriction, degradation, erasure or destruction of information;
d) Sharing with, transfer and further processing, to and with such information.

"Record" means any recorded information—

a) Regardless of form or medium, including any of the following:
    (i) Writing on any material;
    (ii) Information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored;
    (iii) Label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;
    (iv) Floor map, plan, graph or drawing;
    (v) Photograph, video, or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced;

b) In the possession or under the control of a Responsible Party;

c) Whether or not it was created by a Responsible Party; and

d) Regardless of when it came into existence.

"Responsible Party" means TriAlpha including without detracting from the generality thereof, its directors, management, executives, HR practitioner, payroll service providers, other benefits provider, provident fund providers, auditors, legal practitioners and compliance officers, company secretary, and all other employees and Operators who need to process a Data Subject's Personal Information for TriAlpha business purposes.

"**Special Personal Information**" includes any information relating to an individual's: ethnicity, gender, religious or other beliefs, political opinions, sexual orientation, medical history, offences committed or alleged to have been committed by that individual, biometric details, and children's details.

3. BACKGROUND AND USES OF PERSONAL INFORMATION

TriAlpha is mainly a fixed-income multi-manager operating in South Africa. For the purposes of carrying out its business and related objectives, TriAlpha does and will from time to time, process Personal Information of living individuals and legal entities including public and private entities.

TriAlpha uses Personal Information in the following business operations:

- *HR*: Payroll, leave application process, provident fund information requirements, recording of staff training, annual SETA reporting, employment equity reporting, return of earnings submissions, identity verification with regards to recruitment processes and termination of employment exit processing.
- *IT*: New user set up, installation of new software/hardware, incident and IT management, backup of information, recovery of information, Business Continuity Plan/Disaster Recovery testing and reporting, office access.
- *Finance*: Company tax related payments, STT submissions, dividend withholding tax payment processing, creditors company details in the processing of invoices, director's renumeration declaration for audit purposes, salaries payments, bonus payments, provident fund contributions, processing of UIF and PAYE payments, credit card reconciliations, maintenance of bank mandates, management accounts and in the maintenance of the authorized signatories list.
- *Investment*: Initial client take on process, product development process, manager selection and ongoing review process, client risk profiling, portfolio construction and implementation (SA long only and hedge fund products), portfolio construction and implementation (international advisory function), ongoing risk management process, fund valuation and reconciliation process, client reporting and feedback presentations, client disinvestment process, fund audit process, investment vehicles (trustee and company) meetings.
- *Marketing*: Website hosting and internet protocols, placement of advertisements, detail disclosed on business cards and letterheads.

- *Office Admin*: File archiving, flight & travel arrangements, maintenance of TriAlpha and juristic representative's registration documents, telephone recordings, asset insurance, professional insurance, purchases of office supplies.
- *Compliance*: Monitoring of conflicts, gifts, personal account dealing, marketing material review, CPD training review, FAIS accreditation and complaints, FAIS compliance, Assets Under Management and financial soundness reporting, audited financial statements submissions to FSCA, maintaining FSP and regulated persons records at the regulator, review of client risk profiling, CIPC returns.
- *B-BBEE Reporting*: Information pertaining to ownership, management control, skills development, procurement, enterprise & supplier development, socio economic development elements of the scorecard for BEE verification.

TriAlpha shares Personal Information inside and/or outside the group with vendors, contractors, custodians, underlying fund managers and administrators that provide business, professional, or technical support functions to us. The service providers are only given access to information to the extent necessary to process information and/or provide services to TriAlpha, and they are prohibited from using or sharing information for any other purposes.

The purpose of this policy is to formalize a process whereby it is ensured that all conditions and measures as set out in the POPIA Act are complied with. This policy is developed by the Information Officer and falls under the purview of the Risk & Compliance Committee oversight function. An updated policy is submitted to this committee if necessary, where internal changes necessitate amendments, and/or as regularly as required by the Act and relevant regulations to ensure it remains fit-for-purpose and adequate given TriAlpha's business operations. Once reviewed by the Risk & Compliance Committee it is tabled at the next board of directors meeting for approval.

4. PROCESSING LIMITATION

TriAlpha processes Personal Information on at least one of the following four legal bases:

4.1. Contract

Personal Information is typically required to fulfil steps linked to a contract, including:

- providing and maintaining our service offering;
- verifying identities, managing client accounts and/or allowing client access to different functionalities that are available to employees or clients of TriAlpha;
- making payments in relation to contractual undertakings;
- communicating with clients to attend and manage client requests.

How we ensure compliance with POPIA:

- Where the rendering of TriAlpha's financial services and corporate operations necessitates the collection of Personal Information, legal agreements are signed with clients, Operators and

employees.

- TriAlpha imposes appropriate security, privacy, and confidentiality obligations on third parties we contract with to ensure that Personal Information that we remain responsible for, is kept secure. We ensure that anyone to whom we pass Personal Information agrees to treat the information with the same level of protection as we are obliged to. Moreover, liability clauses are specifically included in existing contracts, to enable claims to be instituted for any loss suffered as a result of the Operator's negligence or breach of POPIA.
- Due Diligence on the Operators are performed to evidence security measures undertaken to safeguard Personal Information processed on behalf of TriAlpha. In addition, measures are also taken to ensure security standards are similar to POPIA where General Data Protection Regulation is applicable. See Annexure H, Operator Due Diligence Questionnaire template.
- The central contract register, which includes details such as business area relatedness and renewal dates, is reviewed on an annual basis to ensure that all contracts in force have the necessary POPIA clauses to give effect to the aforementioned. Findings of this annual process is shared with the Risk & Compliance Committee and the board of directors through the Personal Information log, this is discussed in more detail under Employee Responsibilities.

4.2. Consent

This includes where consent is:

- required by applicable law, such as direct marketing in relation to our relevant product and services;
- requested where data is used for a specific purpose; or
- is compatible with the purpose for which we originally collected Personal Information and where such use is lawful.

How we ensure compliance with POPIA:

- Where consent is granted, evidence is documented in the form of signed client consent and employee consent. For templates in this regard, see Annexure B and C.
- Further specific business process implications are listed below:
  - *HR*: POPIA Employee Agreement and Consent Declaration was distributed for current employees' signature and incorporated into future employment contracts.
  - *Investment*: POPIA Client Agreement and Consent Declaration was distributed for clients' signature and incorporated into investment management agreement pack as an annexure.

4.3. Legal Obligation

This includes:

- in response to requests by government or law enforcement authorities conducting an investigation;
- using Personal Information in connection with legal claims, compliance, regulatory and investigative

purposes as necessary, including disclosure of such information in connection with legal process or litigation.

How we ensure compliance with POPIA:

- Privacy Policy, POPIA manual to accessing information (Annexure E) and PAIA Form C (Annexure F) are published on our website.

4.4. Legitimate Interests

To pursue our legitimate interests:

- in marketing our business,
- ensuring that we conduct our business in line with our objectives,
- improving and developing our products and services, and
- keeping our records accurate and up to date.

How we ensure compliance with POPIA:

- Where lawful grounds for processing is of a legitimate interest, a legitimate interest assessment is conducted and documented. See Annexure A, for a template in this regard.
- Further specific business process implications are as follows:
  - *Investment*: The head of department signs off on legitimate impact assessments for client interest, product development and manager selection. This occurs prior to product launch, or initiation of client on-boarding process, or when a manager due diligence process is undertaken.
  - *Marketing:* A legitimate impact assessment for branding, letterhead, business cards, website hosting and branding is carried out.
  - *Office Admin:* Head of business area signs off on legitimate impact assessments for telephone recordings and biometric information storage.

5. DATA RETENTION

We retain Personal Information for as long as we have a relationship with a Data Subject or for a period of time after the end of a relationship which enables us to:

- Maintain business records for analysis and/or audit purposes;
- Comply with record retention requirements under the law;
- Defend or bring any existing or potential legal claims;
- Address any complaints regarding the services;
- Enforce our employment and service agreements;
- Support our legitimate interests, as described in this Policy.

Annexure D provides data retention schedule guideline business divisions heads use to determine whether the retention period is still relevant.

Once TriAlpha is no longer authorised to keep Personal Information, relevant business units will, as part of

the annual business division review process outlined above in the preceding section, take one of the following actions:

- destroy the information;
- delete the information in such a way that it cannot be recovered; or
- de-identify the information in a manner that cannot be reconstructed or used to identify the Data Subject.

A summary of the actions undertaken to give effect to the aforementioned will be included in the Personal Information log that will be submitted to the Information Officer on a yearly basis by all business divisions heads.

6. SECURITY SAFEGUARDS

6.1. Information Technology Security Controls

TriAlpha's networks, systems and devices are actively managed to prevent unauthorised access to Personal Information on TriAlpha's systems. A summary is given below:

INFORMATION TECHNOLOGY SECURITY CONTROLS	
FIRMWARE AND SUBSCRIPTIONS	Vendor support is prioritized to obtain the latest security notifications, updates (including server updates), and configuration management best practices. Latest compatible firmware is installed on all members of the security fabric.
NETWORK DESIGN AND POLICIES	TriAlpha's business and risk driven network security architecture ensures that only authorized business users and traffic are permitted to access network resources. Configuration design takes into account enterprise security and compliance requirements, as well as industry accepted standards for enterprise security. TriAlpha's defence strategies include the following: 1. Authorized access layer devices 2. Secure Wireless Connections 3. Regular review of Firewall policies. Unused policies are disabled and logged. 4. Segregation of traffic

	5. VLAN Change Management. Identification of interfaces on firewalls that are directly connected to 3rd party switches. 6. Use of compatible NAT and third-party router 7. Interface classification 8. Device Discovery. Network topology and device movement is monitored and reported. 9. Interface Classification 10. Detection of Botnet Connections 11. Explicit Interface Policies 12. Secure Remote Access 13. Double Network Address Translation
SECURITY FABRIC HARDENING	Vendor default configurations, default accounts, passwords and management settings are removed. All unnecessary and insecure services and protocols should are disabled. Only business justified services and protocols are permitted, logged and reviewed on a regular basis. 1. Unsecure Management Protocols 2. Change the Admin Account 3. Valid HTTPS Certificate - Administrative GUI 4. Valid HTTPS Certificate - SSLVPN 5. Administrator Password Policy 6. Potentially Insecure Policies, logical Policies, Fabric Policy Consistency 7. Access Control and Authentication. Encrypted corporate mobile phone devices and laptops
THREAT AND VULNERABILITY MANAGEMENT	All network and user devices to be scanned for weaknesses on a regular basis to detect and prevent current and evolving malicious software threats using the following: 1. Advanced Threat Protection 2. Endpoint Quarantine 3. Network Anti-Virus 4. Host based Intrusion Prevention 5. Protection from Malicious Websites 6. Detect Malicious Applications 7. Unified Threat Management Inspection Optimization

ENDPOINT MANAGEMENT	TriAlpha prioritizes following: 1. Endpoint Registration and Vulnerabilities 2. Endpoint Compliance All end user and server systems should comply with security and acceptable use policies, to ensure that users and applications activity are monitored and prevented from connecting to unauthorized and unsafe resources. Only approved applications are be permitted to run on end user systems and access critical network resources.
AUDIT LOGGING AND MONITORING	All user and traffic activity is tracked and verified based on business priorities basis. Evidence is collected to demonstrate conformance with Regulatory and other standards requirements.

TriAlpha's infrastructure is designed and maintained to

- promptly discover a cyber-attack and effectively eradicate an attacker's presence, and
- restore the integrity of the network and systems.

TriAlpha regularly tests the effectiveness of physical and system security as outlined in the Business Continuity Plan. We also systematically employ the expertise of independent third parties to review and identify gaps within the environment so that we can strengthen internal controls for ongoing monitoring, should any deficiencies be identified.

6.2. Code of Conduct

The code of conduct of TriAlpha Employees with respect to security is as follows:

- Do not share network passwords, access codes or rights with anyone.
- Lock your computer screen whenever you step away from your desk.
- Shut down your laptop at the end of the day.
- Adhere to the clear desk rule. Furthermore, ensure Personal Information is not on post-it notes left as reminders around your desk.
- Only password protected document containing personal information should be transmitted between TriAlpha and a third party.
- Only share the Guest Wi-Fi with office visitors.
- Exercise due care and attention to suspicious emails and if in doubt report to IT as a potential phishing attack.
- Collect items sent for printing immediately from the relevant machine.
- Ensure all Personal Information is locked away at the end of the day.

- All archiving to be clearly labelled and destruction dates identified.
- Use offsite archiving wherever possible with appropriate controls.
- Report loss of corporate phone, laptop, any Personal Information immediately to the IT business unit and the Risk and Compliance Committee in line with the procedures set out in the Privacy and Protection of Personal Information Policy.
- Always keep storage facilities for Personal Information locked.

End user security awareness and training is conducted periodically to highlight social engineering and spear-phishing attacks.

6.3. Management Control

- Quarterly IT SLA meetings held to discuss in detail electronic security protocols and their performance with regards to protecting the network from threats.
- Senior management reports any loss of corporate equipment to the Risk and Compliance Committee.

7. EMPLOYEE RESPONSIBILITIES

- All employees have the responsibility to ensure that Personal Information is updated accurately, across relevant business areas once made aware of changes to Personal Information and must inform relevant Operators.
- Business division heads are required to inform Data Subjects of his/her rights to access his/her information and provide Data Subjects with the ability to object to the processing of their Personal Information.
- All employees have an obligation to notify the Information Officer immediately if they believe that there has been a data breach. In the event of a breach and Personal Information has been accessed or acquired by any unauthorized party, the Information Officer is required to notify the Information Regulator. The Data Subject needs to receive formal notification of this fact. The notification to the Data Subject must be provided with extreme haste and with sufficient information to allow the subject to protect themselves against the possible consequences of the Personal Information falling into the wrong hands.
- All business division heads are required to keep a Personal Information log that sets out the purpose for which Personal Information is gathered. Once a year, in a period determined by the Information Officer, business division heads are required to review the Personal Information log to ensure whether a legal basis still exists to hold such information and whether the Personal Information is still accurate. Business divisions are required to destroy Personal Information in a manner that prevents its reconstruction if authorization no longer exists. If any errors are found these need to be corrected immediately and incidents need to be registered in the Personal Information log. This review process will form the basis of the business division POPIA report, which will be submitted to the Information Officer as soon as the review process has been concluded. The business division

POPIA report will also provide a summary of specific POPIA related actions instituted over the review period as per the guidelines provided above. The Information Officer will collate the business division POPIA reports and once finalized will formulate an overarching POPIA adequacy report that will be tabled at the Risk & Compliance Committee and the board of directors' meetings at least once during a calendar year.

- Regular training to staff is also provided to promote a culture of observing data security, confidentiality practices and highlight to employees the importance of being cognizant of Further Processing Limitations. Ideally training will coincide with the period the Information Officer identifies for the Personal Information logs to be updated.

8. DATA SUBJECT PARTICIPATION

In terms of POPIA, a Data Subject may be eligible to

(a) ask us for a copy of Personal Information;

(b) correct, delete or restrict processing of Personal Information; and

(c) obtain the Personal Information provided to us in a structured, machine readable format.

In addition, Data Subjects may have the right under applicable law to object to the processing of Personal Information in some circumstances.

Other South African Data Subjects Rights

South African Consumer Protection Act, No 68 of 2008

South Africa law gives South African consumers the right to opt-out of direct marketing using Personal Information. TriAlpha does not sell Personal Information.

Promotion of Access to Information Act, No. 2 of 2000

A requester can ask for a record held by TriAlpha in pursuant to exercise or protect any right. The request will be at a prescribed fee listed on Annexure G (may be levied before the actual record or description of the Personal Information is made available to the Data Subject). The requester must clearly state the nature of the right(s) that they are seeking to protect or enforce by means of the records requested. Where a request is made, TriAlpha is obliged to provide confirmation free of charge to Data Subjects that we hold Personal Information and will release the information except where the Act expressly provides that the information may or must not be released.

Rights regarding Personal Information may be limited, for example, if fulfilling a request would reveal Personal Information about another person or would infringe the rights of a third party (including our rights), or if we are asked to delete information which we are required by law to keep or have compelling legitimate interests in keeping. We will inform the requester in writing within a reasonable time of the relevant exemption upon which we rely when responding to any requests made. If a request is denied by our Information Officer, the requester is entitled to apply to a court with appropriate jurisdiction for relief.

Our use of certain Personal Information is necessary for us to provide information about our services or

potential employment.

If a Data Subject believes his/her rights regarding Personal Information have been infringed upon, the Data Subject can contact us at +27 (0) 21 809 1210. If a Data Subject wishes to receive or delete information as described in this section, a Promotion of Access to Information Act Form C stored under the Public Documents link on the TriAlpha Website can be completed and sent to us to request such action.

Employees of TriAlpha, are requested to update Personal Information through internal procedures.

9. ADDITIONAL INFORMATION

Third-party Content

Our website may also offer Data Subjects the ability to interact with content provided by third parties not affiliated with TriAlpha ("third-party content"). Third-party content linked to or embedded on the website is governed by the privacy policies of those third parties. Data Subjects use of third-party content is subject to each site's privacy policy, which may be different from ours. We have no control over the information that is collected, stored, or used by third-party content.

Questions or Concerns about this Privacy Policy

Whenever we receive a formal complaint, we make best efforts to contact the person who made the complaint to attempt to resolve their concerns. Should Data Subjects have any questions about the use of Personal Information, or the contents of this Privacy Policy, please contact us.

Questions or concerns regarding this Privacy Policy can be directed to privacy@trialpha.co.za. Clients may also have the right to file a complaint with South Africa's information regulator https://www.justice.gov.za/inforeg/.

Amendments to this Policy

We review this Privacy Policy and reserve the right to make changes to this Privacy Policy at any time. If we do make material changes, we will give notice via the website features.

10. CONTACT DETAILS

Any questions please can be directed to the Information Officer, using the below contact above.

Head Office	
Telephone Number	+27 (0) 21 809 1210
Physical Address	Room 12B, 2nd Floor Ou Kollege Building Stellenbosch South Africa 7600
Postal Address	Postnet Suite Number 227 Private Bag X5061 Stellenbosch South Africa 7599
Email address	privacy@trialpha.co.za
Information Officer	Prudence Lebina
Deputy Information Officer	Simphiwe Khumalo