POLICY STATEMENT AND MANUAL

Protection of Personal Information (POPIA)

FOR

FOURTH DIMENSION FINANCIAL SERVICES (PTY) LTD

and all its subsidiaries and affiliated companies

(Hereinafter referred to as 4D)

1. Introduction and Purpose

4D is a company functioning within the Financial Services sector that is obligated to comply with The Protection of Personal Information Act 4 of 2013.

POPIA requires 4D to inform the consumer as to the manner in which their personal information is used, protected, disclosed and destroyed.

4D guarantees its commitment to protecting the consumer's privacy and ensuring that their personal information is used appropriately, transparently, securely and in accordance with applicable laws.

This Policy sets out the manner in which 4D deals with the consumer's personal information and stipulating the purpose for which said information is used.

The Policy will be made available on the 4D website at www.4D.co.za and by requesting it from the 4D's head office.

The purpose of this policy is to inform consumers and enable 4D to comply with The laws in respect of personal information, it holds about data subjects

- **Follow good practice**
- **Protect 4D's reputation**
- **Protect 4D from the consequences of a breach of its responsibilities**
- **Protect the Consumer against loss or breach of their personal information.**

2. Background

The Protection of Personal Information Act 4 of 2013 is one of the high reputational risk legislations 4D must comply with. The purpose of this legislation is to regulate the processing of personal information by public and private bodies. This policy applies to information relating to identifiable individuals, in terms of the Protection of Personal Information Act, 2013 (hereinafter POPIA Act).

3. Definitions

Data subject means the person to whom personal information relates

POPIA refers to the Protection of Personal Information Act 4 of 2013

Processing means 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.

Record means any recorded information) regardless of form or medium, including any of the following

- writing of any material
- information produced, recorded or stored by means of any tape-recorder, computer equipment,
    a) whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means: book, map, plan, graph or drawing, photograph, film, negative, tape 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 in the possession or under the control of a responsible party
    b) whether or not it was created by a responsible party and
    c) regardless of when it came into existence.

Responsible party means a public or private body or any other person which, alone or in conjunction with others determines the purpose of and means for processing personal information.

Personal Information means 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, wellbeing, 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
    a) the biometric information of the person
    b) the personal opinions, views or preferences of the person
    c) 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
    d) the views or opinions of another individual about the person and
    e) 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

4. Policy Statement and Responsibilities

4D guarantees its commitment to protecting the client and consumer's privacy and ensuring their Personal information is used appropriately, transparently, securely and in accordance with applicable laws, as far as it applies to our specific industry.

5. Compliance with regard to Protection of Personal Information.

Data subjects has the following rights.

- Objection to the use of personal information.
- Notification if information is being used for something other than what was consented for.
- Establishing whether the responsible party holds information.
- Request that information can be corrected, destructed or deleted.
- Refuse processing for direct marketing by unsolicited electronic communications.
- Lodge a complaint with the Information Regulator.
- Institute civil proceedings. (Sec 99)

Conditions for lawful processing

- **Accountability**
  The Responsible party must ensure that the conditions set out in the Act and all the measures that give effect to such conditions, are complied with at the time of the determination of the purpose and means of the processing and during the processing itself.

- **Processing Limitations**
  Data subjects must consent.
  Consent is necessary to carry out actions to conclude or perform a contract to which the data subject is a party.
  Processing compliance with an obligation imposed by law.
  Must process to protect the legitimate interest of data subject.
  For proper performance of public law duty by a public body.
  Pursue legitimate interest of other responsible party or third party to whom the information was supplied.
  Data subject may withdraw consent.
  Data subject may object on reasonable grounds.

- **Specific Purpose**
  Personal Information must be collected for a specific, explicitly defined and lawful purpose related to the function or activity of the responsible party.
  The data subject must be made aware of the purpose of the collection.
  Records must not be retained any longer than is necessary for achieving the purpose for which it was collected unless:
  - further retention is required by law.
  - the responsible party is reasonably required to keep it.
  - retention is required by a contract between the parties.

- the data subject consents to the further retention.
- Personal Information must be destroyed, deleted or de-identified as soon as is reasonably practical. Destruction or deletion must be done in a manner that prevents its reconstruction in an intelligible form.
- The information officer shall ensure that the information collected will not be used for any other purpose before obtaining the individual's approval, unless the new purpose is required by law.
- The information officer shall ensure that a person collecting personal information will be able to explain to the individual why this is being done.
- The Information officer shall ensure that limited collection, limited use, disclosure, and retention principles are respected in identifying why personal information is to be collected.

- **Limiting collection and further processing**
    a) Must be in accordance or compatible with the purpose for which it was collected.
    b) The Responsible Party shall ensure that personal information will not be collected indiscriminately, but by fair and lawful means, and be limited to what is necessary to fulfil the specific purpose for which the Personal Information is being collected.

    Personal Information may only be processed if:
        - the data subject consents to the processing.
        - processing is necessary for the conclusion or performance of a contract to which the data subject is a party.
        - there is a legal obligation to do the processing.
        - processing protects the legitimate interests of the data subject.
        - processing is necessary for the proper performance of a public law duty by a public body.
        - processing is necessary for the pursuit of legitimate interests of the responsible party.
        - A data subject may object, at any time, on reasonable grounds, to the processing of their Personal information. The responsible party may then no longer process the Personal information.

    Personal Information must be collected directly from the data subject except if:
        - the information is contained in a public record or has deliberately been made public by the data subject.
        - the data subject has consented to the collection from another source.
        - collection from another source would not prejudice a legitimate interest of the data subject.
        - Collection from another source is necessary:
        - to maintain law and order
        - to enforce legislation concerning the collection of revenue
        - for the conduct of court or tribunal proceedings
        - in the interests of national security
        - to maintain the legitimate interests of the responsible party
        - compliance would prejudice a lawful purpose of the collection; or
        - compliance is not reasonably practicable in the circumstances of the particular case.

- Further processing must be compatible with the purpose for which it was collected, unless the data subject gives consent to the further processing.

- **Information quality**
  a) Information must be complete, accurate, not misleading and updated where necessary.

- **Openness**

4D must take reasonably practicable steps to ensure the Data Subject is aware of:

b) the information being collected.
c) the name and address of the Responsible Party.
d) the purpose for which the information is being collected.
e) whether or not the supply of the information is voluntary or mandatory.
f) the consequences of failure to provide the information.
g) any particular law authorising the requiring of the collection.
h) the right of access to and the right to rectify the information collected.
i) the fact that, where applicable, the responsible party intends to transfer the information to a third country/international organisation and the level of protection afforded by that third country/organisation; and
j) the right to object to the processing of the information. This must be done prior to collecting Personal information if the Personal information is collected directly from the data subject, or in any other case as soon as is reasonably practical after collection.

- **Security Safeguards**
  a) Responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical organisational measures.

Anyone processing Personal information on behalf of a responsible party must:

- treat the information as confidential and not disclose it unless required by law;
- apply the same security measures as the responsible party;
- the processing must be governed by a written contract ensuring safeguards are in place; and
- if domiciled outside the Republic, comply with local protection of personal information laws.

The Data Subject may request responsible party to:

- correct or delete Personal information that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully.
- delete or destroy Personal information that the responsible party is no longer authorised to retain.
- The Officer shall ensure that all employees and volunteers know the importance of keeping personal information confidential.
- The Officer shall ensure that care is taken when personal information is disposed of or destroyed to prevent unauthorized parties from gaining access to it.
- Responsible party should notify data subject and Regulator of any breach of data.

6. Information Regulator

- It has jurisdiction throughout the Republic of South Africa.
- Is independent and is subject only to the Constitution.
- Must exercise its powers and perform its functions in accordance with the Act and Promotion of access to Information Act and
- Is accountable to the National Assembly.
- Enforces Offences and Penalties.
- Minor Offences imposed by the Regulator can be a fine and/or imprisonment up to 12 months.
- Major Offences imposed by the Regulator can be a fine and/or imprisonment up to 10 years.

7. Information Officer Responsibilities

The Core focus or duties under POPIA for the Information officer will be the following, but not limited to:

- Encourage compliance with the information protection conditions in terms of Section 55 of POPIA.
- Developing, publishing and maintaining a POPIA Policy which addresses all relevant provisions of the POPIA Act.
- Reviewing the POPIA Act and periodic updates as published.
- Ensuring that POPIA Act induction training takes place for all staff.
- Ensuring that periodic communication awareness on POPIA Act responsibilities takes place.
- Ensuring that Privacy Notices for internal and external purposes are developed and published.
- Handling data subject access requests.
- Approving unusual or controversial disclosures of personal data.
- Approving contracts with Data Operators.
- Ensuring that appropriate policies and controls are in place for ensuring the information quality of Personal information.
- Ensuring that appropriate Security Safeguards in line with the POPIA Act for personal information are in place.
- Consider requests made pursuant to POPIA.
- Work with the Regulator in relation to investigations conducted pursuant to Chapter 6 against 4D.
- Identify and govern all privacy related risks.
- Map all activities performed concerning the collection and storage of Personal information.
- Map all privacy laws and industry codes relevant to our activities.
- If applicable, know, understand, and ensure corporate compliance with all relevant laws of foreign jurisdictions in which we conduct business.
- Coordinate the development, implementation, and maintenance of corporate customer (external) and employee (internal) privacy policies.
- Ensure compliance with corporate privacy policies and procedures throughout the body.
- Liaise with Human Resources and Legal Departments to ensure standards of disciplinary action and sanction for non-compliance.
- Create standards or scripts for responding to customer or public enquiries.
- Create and implement procedures and standards to facilitate customer verification of captured and stored personal information files.

- Monitor and control the privacy requirements and responsibilities of information processing service providers or operators in terms of sections 20 and 21 of POPIA.
- Manage breach and incident investigation processes.
- Create and implement our privacy breach management plan, privacy alerts, and other privacy related operational issues.
- Create standards and procedures to manage any compromise in the security of the stored personal information correctly and appropriately.
- Investigate, analyse and document all privacy related incidents and complaints.
- Apply investigation findings to update standards, processes and systems as an on-going operational improvement routine.

8. Trans border Information flows.

a) Scope

- The scope of this aspect of the policy is defined by the provisions of the POPIA Act Chapter 9.

b) Trans border Information flows.

- 4D will ensure that the POPIA Act Chapter 9, section 72 is fully complied with.
- Compliance with section 72 will be achieved through the use of the necessary contractual commitments from the relevant third parties.

9. Safeguarding client information.

It is a requirement of POPIA to adequately protect the Personal Information we hold and to avoid unauthorized access and use of your Personal information. We will continuously review our security controls and processes to ensure that your Personal Information is secure.

The following procedures are in place in order to protect the consumer's Personal Information:

- The 4D Group information officer is Laurika du Plessis whose details are available below and who is responsible for compliance with the conditions of the lawful processing of personal information and other provisions of POPIA.
- This Policy has been put in place throughout the 4D Group and training on this policy and the POPIA Act have already taken place and will take place during 2020/21.
- The 4D Group has done a risk assessment to determine where the risk to our clients lie.
- We have identified the relevant role players and appointed the correct people to safeguard your personal information, we have mapped our activities, recorded how to process lawfully and have implemented the correct action items.
- We have identified quick wins and have implemented the following:
    - Incident Response Policy.
    - Privacy Policy.
    - PAIA Manual.
    - POPIA Policy.
    - Awareness Training and risk assessment.
    - We have implemented access control.
    - We have proper Non-Disclosure agreements and Service Level Agreements in place.

- We have security in place with regard to Memory Sticks, USB Ports, Mobile Devices and Shredders of documents.

- Each new employee will be required to sign an Employment Contract containing relevant clauses for these and storage of employee information, or any other action so required, in terms of POPIA.
- Every employee currently employed within the 4D Group will be required to sign an addendum to the Employment Contracts containing relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of POPIA.
- Our current client information is stored on site and by a third-party Service Provider, who has been evaluated by our Directors and Group Compliance have established that storage complies with the Act.
- Our Clients and third party service providers will be required to sign a Service Level Agreement guaranteeing their commitment to the Protection of personal Information.
- The 4D Group captures all files electronically for back up purposes. All files will be archived offsite which will be available in case of a breach.
- All electronic files or data are backed up by the Group IT Service Provider who is also responsible for system security which protects third party access and physical threats.

10. Scope

- The scope of this aspect of the policy is written in support of the provisions of the POPI Act, Chapter 5, Part B.
- The 4D Information Officer will ensure that all staff that has access to any kind of personal information will have their responsibilities outlined during their induction procedures.
- Continuing training will provide opportunities for staff to explore POPIA Act issues through training, team meetings, and supervisions.
- Procedure for staff signifying acceptance of this policy 4D will ensure that all staff sign acceptance of this policy once they have had a chance to understand the policy and their responsibilities in terms of the policy and the POPIA Act.

11. Policy review.

- The 4D Information Officer is responsible for an annual review to be completed prior to the policy anniversary date.
- The 4D Information Officer will ensure relevant stakeholders are consulted as part of the annual review to be completed prior to the policy anniversary date.

12. Details of Information officer

Name: Laurika Du Plessis
Telephone Number: (012) 991 9600
Postal Address: PO Box 73481, Lynnwood Ridge, Pretoria 0040
Physical Address: 107 Haymeadow Crescent, Boardwalk Office Park, 4D House Block 2, Ground floor, Faerie Glen, 0043