



***PRIVACY POLICY IN TERMS OF THE PROTECTION OF PERSONAL
INFORMATION ACT FOR SPIDDI INVESTMENTS***

Document Version Control and Revision History:

Version	Date	Author	Summary of changes
1.0	1 JAN 2025	NTISETSO MOLOI	FIRST DRAFT
1.1	1 JAN 2026		Change only if necessary
1.2	1 JAN 2027		Change only if necessary

This document has been adopted as follows:

	Responsibility	Signature	Date
Drafted by:	NTISETSO MOLOI HEAD OF INFORMATION AND COMMUNICATION TECHNOLOGY		01/01/2026
Reviewed by:	SITHENGIWE NTONGA HEAD OF LEGAL RISK AND COMPLIANCE		01/01/2026
Approved by:	INNOCENT SHABALALA CHIEF EXECUTIVE NON-EXCO BOARD MEMBER AND SHAREHOLDER		01/01/2026

TABLE OF CONTENTS

1. INTRODUCTION.....	Page 6
2. DEFINITIONS.....	Page 7
2.1 Personal Information.....	Page 7
2.2 Data Subject.....	Page 8
2.3 Responsible Party.....	Page 9
2.4 Operator.....	Page 9
2.5 Information Officer.....	Page 9
2.6 Processing.....	Page 10
2.7 Record.....	Page 11
2.8 Filing System.....	Page 12
2.9 Unique Identifier.....	Page 12
2.10 De-Identify.....	Page 12
2.11 Re-Identify.....	Page 13
2.12 Consent.....	Page 13
2.13 Direct Marketing.....	Page 14
2.14 Biometrics.....	Page 14
3. POLICY PURPOSE.....	Page 14
4. POLICY APPLICATION.....	Page 16
5. RIGHTS OF DATA SUBJECTS.....	Page 17
5.1 The Right to Access Personal Information.....	Page 18
5.2 The Right to have Personal Information Corrected or Deleted.....	Page 18
5.3 The Right to Object to the Processing of Personal Information.....	Page 18
5.4 The Right to Object to Direct Marketing.....	Page 19
5.5 The Right to Complain to the Information Regulator.....	Page 19
5.6 The Right to be Informed.....	Page 20
6. GENERAL GUIDING PRINCIPLES.....	Page 20
6.1 Accountability.....	Page 20
6.2 Processing Limitation.....	Page 21

6.3 Purpose Specification.....	Page 22
6.4 Further Processing Limitation.....	Page 23
6.5 Information Quality.....	Page 23
6.6 Open Communication.....	Page 24
6.7 Security Safeguards.....	Page 25
6.8 Data Subject Participation.....	Page 27
7. INFORMATION OFFICERS.....	Page 27
8. SPECIFIC DUTIES AND RESPONSIBILITIES.....	Page 28
8.1 Governing Body.....	Page 28
8.2 Information Officer.....	Page 30
8.3 IT Manager.....	Page 32
8.4 Marketing & Communication Manager.....	Page 33
8.5 Employees and other Persons acting on behalf of Spiddi	Page 34
9. POPI AUDIT.....	Page 40
10. REQUEST TO ACCESS PERSONAL INFORMATION.....	Page 42
11. POPI COMPLAINTS PROCEDURE.....	Page 43
12. DISCIPLINARY ACTION.....	Page 45
13. ANNEXURE D: EMPLOYEE CONSENT AND CONFIDENTIALITY CLAUSE.....	Page 47
14. ANNEXURE E: SLA CONFIDENTIALITY CLAUSE.....	Page 51

1. INTRODUCTION



- a) The right to privacy is an integral human right recognised and protected in the South African Constitution and in the Protection of Personal Information Act 4 of 2013 ("POPIA").
- b) POPIA aims to promote the protection of privacy through providing guiding principles that are intended to be applied to the processing of personal information in a context-sensitive manner.
- c) Through the provision of quality goods and services, Spiddi Investments is necessarily involved in the collection, use and disclosure of certain aspects of the personal information of clients, customers, employees and other stakeholders.
- d) A person's right to privacy entails having control over his or her personal information and being able to conduct his or her affairs relatively free from unwanted intrusions.
- e) Given the importance of privacy, Spiddi Investments is committed to effectively managing personal information in accordance with POPIA's provisions.

2. DEFINITIONS

2.1 Personal Information

2.1.1 Personal information is any information that can be used to reveal a person's identity. Personal information relates to an identifiable, living, natural person, and where applicable, an identifiable, existing juristic person (such as a company), including, but not limited to information concerning:

- a) race, gender, sex, pregnancy, marital status, national or ethnic origin, colour, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language and birth of a person;
- b) information relating to the education or the medical, financial, criminal or employment history of the person;
- c) any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other 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;
- 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.

2.2 Data Subject

This refers to the natural or juristic person to whom personal information relates, such as an individual client, customer or a company that supplies Spiddi Investments with products or other goods.

2.3 Responsible Party

The responsible party is the entity that needs the personal information for a particular reason and determines the purpose of and means for processing the personal information. In this case, Spiddi Investments is the responsible party.

2.4 Operator

An operator means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party. For example, a third-party service provider that has contracted with Spiddi Investments to shred documents containing personal information. When dealing with an operator, it is considered good practice for a responsible party to include an indemnity clause.

2.5 Information Officer



- a) The Information Officer is responsible for ensuring Spiddi Investments's compliance with POPIA.
- b) Where no Information Officer is appointed, the head of Spiddi Investments will be responsible for performing the Information Officer's duties.
- c) Once appointed, the Information Officer must be registered with the South African Information Regulator established under POPIA prior to performing his or her duties. Deputy Information Officers can also be appointed to assist the Information Officer.

2.6 Processing

The act of processing information includes any activity or any set of operations, whether by automatic means, concerning personal information and includes:

- 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 any restriction, degradation, erasure or destruction of information.

2.7 Record

Means any recorded information, regardless of form or medium, including:

- a) Writing on any material;
- b) 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;

- c) Label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;
- d) Book, map, plan, graph or drawing;
- e) 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.

2.8 Filing System

Means any structured set of personal information, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria.

2.9 Unique Identifier

Means any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party.

2.10 De-Identify

This means to delete any information that identifies a data subject, or which can be used by a reasonably foreseeable method to identify, or when linked to other information, that identifies the data subject.

2.11 Re-Identify

In relation to personal information of a data subject, means to resurrect any information that has been de-identified that identifies the data subject, or can be used or manipulated by a reasonably foreseeable method to identify the data subject.

2.12 Consent

Means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.

2.13 Direct Marketing

Means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of:

- a) Promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject;
or
- b) Requesting the data subject to donate any kind for any reason.

2.14 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.

3. POLICY PURPOSE

3.1 This purpose of this policy is to protect the Spiddi Investments from the compliance risks associated with the protection of personal information which includes:

- a) Breaches of confidentiality. For instance, Spiddi Investments could suffer loss in revenue where it is found that the personal information of data subjects has been shared or disclosed inappropriately.
- b) Failing to offer choice. For instance, all data subjects should be free to choose how and for what purpose Spiddi Investments uses information relating to them.

- c) Reputational damage. For instance, Spiddi Investments could suffer a decline in shareholder value following an adverse event such as a computer hacker deleting the personal information held by Spiddi Investments.

3.2 This policy demonstrates the Spiddi Investment's commitment to protecting the privacy rights of data subjects in the following manner:

- a) Through stating desired behaviour and directing compliance with the provisions of POPIA and best practice.
- b) By cultivating an organisational culture that recognises privacy as a valuable human right.
- c) By developing and implementing internal controls for the purpose of managing the compliance risk associated with the protection of personal information.
- d) By creating business practices that will provide reasonable assurance that the rights of data subjects are protected and balanced with the legitimate business needs of Spiddi Investments.
- e) By assigning specific duties and responsibilities to control owners, including the appointment of an Information Officer and where necessary, Deputy Information Officers to protect the interests of Spiddi Investments and data subjects.
- f) By raising awareness through training and providing guidance to individuals who process personal information so that they can act confidently and consistently.

4. POLICY APPLICATION

4.1 This policy and its guiding principles applies to:

- a) The Spiddi Investment's governing body
- b) All branches, business units and divisions of Spiddi Investments
- c) All employees and volunteers
- d) All contractors, suppliers and other persons acting on behalf of Spiddi Investments.



4.2 The policy's guiding principles find application in all situations and must be read in conjunction with POPIA as well as Spiddi Investment's PAIA Policy as required by the Promotion of Access to Information Act (Act No 2 of 2000).

4.3 The legal duty to comply with POPIA's provisions is activated in any situation where there is:

- a) A **processing** of
- b) **personal information**
- c) entered into a **record**
- d) by or for a **responsible person**
- e) who is **domiciled** in South Africa.

4.4 POPIA does not apply in situations where the processing of personal information:

- a) is concluded during purely personal or household activities, or
- b) where the personal information has been de-identified.

5 RIGHTS OF DATA SUBJECTS

- a) Where appropriate, Spiddi Investments will ensure that its clients and customers are made aware of the rights conferred upon them as data subjects.
- b) Spiddi Investments will ensure that it gives effect to the following seven rights.

5.1 The Right to Access Personal Information

The organisation recognises that a data subject has the right to establish whether the organisation holds personal information related to him, her or it includes the right to request access to that personal information.

An example of a "Personal Information Request Form" can be found under Annexure A.

5.2 The Right to have Personal Information Corrected or Deleted

The data subject has the right to request, where necessary, that his, her or its personal information must be corrected or deleted where Spiddi Investments is no longer authorised to retain the personal information.

5.3 The Right to Object to the Processing of Personal Information

- a) The data subject has the right, on reasonable grounds, to object to the processing of his, her or its personal information.
- b) In such circumstances, Spiddi Investments will give due consideration to the request and the requirements of POPIA. Spiddi Investments may cease to use or disclose the data subject's personal information and may, subject to any statutory and contractual record keeping requirements, also approve the destruction of the personal information.

5.4 The Right to Object to Direct Marketing

The data subject has the right to object to the processing of his, her or its personal information for purposes of direct marketing by means of unsolicited electronic communications.

5.5 The Right to Complain to the Information Regulator

The data subject has the right to submit a complaint to the Information Regulator regarding an alleged infringement of any of the rights protected under POPIA and to institute civil proceedings regarding the alleged non-compliance with the protection of his, her or its personal information.

An example of a "POPI Complaint Form" can be found under Annexure B.

5.6 The Right to be Informed



- a) The data subject has the right to be notified that his, her or its personal information is being collected by Spiddi Investments.
- b) The data subject also has the right to be notified in any situation where Spiddi Investments has reasonable grounds to believe that the personal information of the data subject has been accessed or acquired by an unauthorised person.

6 GENERAL GUIDING PRINCIPLES

All employees and persons acting on behalf of Spiddi Investments will always be subject to, and act in accordance with, the following guiding principles:

6.1 Accountability

- a) Failing to comply with POPIA could potentially damage Spiddi Investment's reputation or expose Spiddi Investments to a civil claim for damages. The protection of personal information is therefore everybody's responsibility.
- b) Spiddi Investments will ensure that the provisions of POPIA and the guiding principles outlined in this policy are complied with through the encouragement of desired behaviour. However, Spiddi Investments will take appropriate sanctions, which may include disciplinary action, against those individuals who through their intentional or negligent actions and/or omissions fail to comply with the principles and responsibilities outlined in this policy.

6.2 Processing Limitation

6.1 Spiddi Investments will ensure that personal information under its control is processed:

- a) in a fair, lawful and non-excessive manner, and
- b) only with the informed consent of the data subject, and
- c) only for a specifically defined purpose.



6.2 Spiddi Investments will inform the data subject of the reasons for collecting his, her or its personal information and obtain written consent prior to processing personal information.

6.3 Alternatively, where services or transactions are concluded over the telephone or electronic video feed, Spiddi Investments will maintain a voice recording of the stated purpose for collecting the personal information followed by the data subject's subsequent consent.

6.4 Spiddi Investments will under no circumstances distribute or share personal information between separate legal entities, associated organisations (such as subsidiary companies) or with any individuals that are not directly involved with facilitating the purpose for which the information was originally collected.

6.5 Where applicable, the data subject must be informed of the possibility that their personal information will be shared with other aspects of Spiddi Investments' business and be provided with the reasons for doing so.

6.6 An example of a "POPI Notice and Consent Form" can be found under Annexure C.

6.3 Purpose Specification

a) All Spiddi Investment's business units and operations must be informed by the principle of transparency.

b) Spiddi Investments will process personal information only for specific, explicitly defined and legitimate reasons. Spiddi Investments will inform data subjects of these reasons prior to collecting or recording the data subject's personal information.

6.4 Further Processing Limitation

a) Personal information will not be processed for a secondary purpose unless that processing is compatible with the original purpose.

b) Therefore, where Spiddi Investments seeks to process personal information, it holds for a purpose other than the original purpose for which it was originally collected, and where this secondary purpose is not compatible with the original purpose, Spiddi Investments will first obtain additional consent from the data subject.

6.5 Information Quality

- a) Spiddi Investments will take reasonable steps to ensure that all personal information collected is complete, accurate and not misleading.
- b) The more important it is that the personal information be accurate (for example, the beneficiary details of a life insurance policy are of the utmost importance), the greater the effort Spiddi Investments will put into ensuring its accuracy.
- c) Where personal information is collected or received from third parties, Spiddi Investments will take reasonable steps to confirm that the information is correct by verifying the accuracy of the information directly with the data subject or by way of independent sources.

6.6 Open Communication

6.6.1 Spiddi Investments will take reasonable steps to ensure that data subjects are notified (are always aware) that their personal information is being collected including the purpose for which it is being collected and processed.

6.6.2 Spiddi Investments will ensure that it establishes and maintains a “contact us” facility, for instance via its website or through an electronic helpdesk, for data subjects who want to:

- a) Enquire whether Spiddi Investments holds related personal information, or
- b) Request access to related personal information, or
- c) Request Spiddi Investments to update or correct related personal information, or
- d) Make a complaint concerning the processing of personal information.

6.7 Security Safeguards



- a) Spiddi Investments will manage the security of its filing system to ensure that personal information is adequately protected. To this end, security controls will be implemented to minimise the risk of loss, unauthorised access, disclosure, interference, modification or destruction.
- b) Security measures also need to be applied in a context-sensitive manner. For example, the more sensitive the personal information, such as medical information or credit card details, the greater the security required.
- c) Spiddi Investments will continuously review its security controls which will include regular testing of protocols and measures put in place to combat cyber-attacks on Spiddi Investments's IT network.
- d) Spiddi Investments will ensure that all paper and electronic records comprising personal information are securely stored and made accessible only to authorised individuals.
- e) All new employees will be required to sign employment contracts containing contractual terms for the use and storage of employee information. Confidentiality clauses will also be included to reduce the risk of unauthorised disclosures of personal information for which Spiddi Investments is responsible.
- f) All existing employees will, after the required consultation process has been followed, be required to sign an addendum to their employment containing the relevant consent and confidentiality clauses.
- g) Spiddi Investment's operators and third-party service providers will be required to enter into service level agreements with Spiddi Investments where both parties pledge their mutual commitment to POPIA and the lawful processing of any personal information pursuant to the agreement.
- h) An example of "Employee Consent and Confidentiality Clause" for inclusion in Spiddi Investments's employment contracts can be found under Annexure D.
- i) An example of an "SLA Confidentiality Clause" for inclusion in the Spiddi Investment's service level agreements can be found under Annexure E.

6.8 Data Subject Participation



- a) A data subject may request the correction or deletion of his, her or its personal information held by Spiddi Investments.
- b) Spiddi Investments will ensure that it provides a facility for data subjects who want to request the correction or deletion of their personal information.
- c) Where applicable, Spiddi Investments will include a link to unsubscribe from any of its electronic newsletters or related marketing activities.

7 INFORMATION OFFICERS

- a) Spiddi Investments will appoint an Information Officer and where necessary, a Deputy Information Officer to assist the Information Officer.
- b) Spiddi Investment's Information Officer is responsible for ensuring compliance with POPIA.
- c) There are no legal requirements under POPIA for an organisation to appoint an Information Officer. Appointing an Information Officer is however, considered to be a good business practice, particularly within larger organisations.
- d) Where no Information Officer is appointed, the head of Spiddi Investments will assume the role of the Information Officer.
- e) Consideration will be given on an annual basis to the re-appointment or replacement of the Information Officer and the re-appointment or replacement of any Deputy Information Officers.
- f) Once appointed, Spiddi Investments will register the Information Officer with the South African Information Regulator established under POPIA prior to performing his or her duties.

An example of an "Information Officer Appointment Letter" can be found under Annexure F.

8 SPECIFIC DUTIES AND RESPONSIBILITIES

8.1 Governing Body



- 8.1.1 Spiddi Investment's governing body cannot delegate its accountability and is ultimately answerable for ensuring that Spiddi Investments meets its legal obligations in terms of POPIA.
- 8.1.2 The governing body may however delegate some of its responsibilities in terms of POPIA to management or other capable individuals.
- 8.1.3 The governing body is responsible for ensuring that:
- a) Spiddi Investments appoints an Information Officer, and where necessary, a Deputy Information Officer.
 - b) All persons responsible for the processing of personal information on behalf of Spiddi Investments:
 - i. are appropriately trained and supervised to do so,
 - ii. understand that they are contractually obligated to protect the personal information they meet, and
 - iii. are aware that a wilful or negligent breach of this policy's processes and procedures may lead to disciplinary action being taken against them.
 - c) Data subjects who want to make enquires about their personal information are made aware of the procedure that needs to be followed should they wish to do so.
 - d) The scheduling of a periodic POPI Audit to accurately assess and review the ways in which Spiddi Investments collects, holds, uses, shares, discloses, destroys and processes personal information.

8.2 Information Officer

Spiddi Investments' Information Officer is responsible for:

- a) Taking steps to ensure Spiddi Investments reasonable compliance with the provision of POPIA.
- b) Keeping the governing body updated about Spiddi Investments information protection responsibilities under POPIA. For instance, in the case of a security breach, the Information Officer must inform and advise the governing body of their obligations pursuant to POPIA.



- c) Continually analysing privacy regulations and aligning them with Spiddi Investments' personal information processing procedures. This will include reviewing Spiddi Investment's information protection procedures and related policies.
- d) Ensuring that POPI Audits are scheduled and conducted on a regular basis.
- e) Ensuring that Spiddi Investments makes it convenient for data subjects who want to update their personal information or submit POPI related complaints to Spiddi Investments. For instance, maintaining a "contact us" facility on Spiddi Investments's website.
- f) Approving any contracts entered with operators, employees and other third parties which may have an impact on the personal information held by Spiddi Investments. This will include overseeing the amendment of Spiddi Investments' employment contracts and other service level agreements.
- g) Encouraging compliance with the conditions required for the lawful processing of personal information.
- h) Ensuring that employees and other persons acting on behalf of Spiddi Investments are fully aware of the risks associated with the processing of personal information and that they remain informed about Spiddi Investments's security controls.
- i) Organising and overseeing the awareness training of employees and other individuals involved in the processing of personal information on behalf of Spiddi Investments.
- j) Addressing employees' POPIA related questions.
- k) Addressing all POPIA related requests and complaints made by Spiddi Investments's data subjects.
- l) Working with the Information Regulator in relation to any ongoing investigations. The Information Officers will therefore act as the contact point for the Information Regulator authority on issues relating to the processing of personal information and will consult with the Information Regulator where appropriate, regarding any other matter.

The Deputy Information Officer will assist the Information Officer in performing his or her duties.

8.3 IT Manager



Spiddi Investment's IT Manager is responsible for:

- a) Ensuring that Spiddi Investment's IT infrastructure, filing systems and any other devices used for processing personal information meet acceptable security standards.
- b) Ensuring that all electronically held personal information is kept only on designated drives and servers and uploaded only to approved cloud computing services.
- c) Ensuring that servers containing personal information are sited in a secure location, away from the general office space.
- d) Ensuring that all electronically stored personal information is backed up and tested on a regular basis.
- e) Ensuring that all back-ups containing personal information are protected from unauthorised access, accidental deletion and malicious hacking attempts.
- f) Ensuring that personal information being transferred electronically is encrypted.
- g) Ensuring that all servers and computers containing personal information are protected by a firewall and the latest security software.
- h) Performing regular IT audits to ensure that the security of Spiddi Investments's hardware and software systems are functioning properly.
- i) Performing regular IT audits to verify whether electronically stored personal information has been accessed or acquired by any unauthorised persons.
- j) Performing a proper due diligence review prior to contracting with operators or any other third-party service providers to process personal information on Spiddi Investments' behalf. For instance, cloud computing services.

8.4 Marketing & Communication Manager

Spiddi Investments' Marketing & Communication Manager is responsible for:



- a) Approving and maintaining the protection of personal information statements and disclaimers that are displayed on Spiddi Investments' website, including those attached to communications such as emails and electronic newsletters.
- b) Addressing any personal information protection queries from journalists or media outlets such as newspapers.
- c) Where necessary, working with persons acting on behalf of Spiddi Investments to ensure that any outsourced marketing initiatives comply with POPIA.

8.5 Employees and other Persons acting on behalf of Spiddi Investments.

8.5.1 Employees and other persons acting on behalf of Spiddi Investments will, during the performance of their services, gain access to and become acquainted with the personal information of certain clients, suppliers and other employees.

8.5.2 Employees and other persons acting on behalf of Spiddi Investments are required to treat personal information as a confidential business asset and to respect the privacy of data subjects.

8.5.3 Employees and other persons acting on behalf of Spiddi Investments may not directly or indirectly, utilise, disclose or make public in any manner to any person or third party, either within Spiddi Investments or externally, any personal information, unless such information is already publicly known or the disclosure is necessary in order for the employee or person to perform his or her duties.

8.5.4 Employees and other persons acting on behalf of Spiddi Investments must request assistance from their line manager or the Information Officer if they are unsure about any aspect related to the protection of a data subject's personal information.

8.5.5 Employees and other persons acting on behalf of Spiddi Investments will only process personal information where:

- a) The data subject, or a competent person where the data subject is a child, consents to the processing; or
- b) The processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party; or
- c) The processing complies with an obligation imposed by law on the responsible party; or

- d) The processing protects a legitimate interest of the data subject; or
- e) The processing is necessary for pursuing the legitimate interests of Spiddi Investments or of a third party to whom the information is supplied.
- f) Furthermore, personal information will only be processed where the data subject:
- g) Clearly understands why and for what purpose his, her or its personal information is being collected; and
- h) Has granted Spiddi Investments with explicit written or verbally recorded consent to process his, her or its personal information.

8.5.6 Employees and other persons acting on behalf of Spiddi Investments will consequently, prior to processing any personal information, obtain a specific and informed expression of will from the data subject, in terms of which permission is given for the processing of personal information.

8.5.7 Informed consent is therefore when the data subject clearly understands for what purpose his, her or its personal information is needed and who it will be shared with.

8.5.8 Consent can be obtained in written form which includes any appropriate electronic medium that is accurately and readily reducible to printed form. Alternatively, Spiddi Investments will keep a voice recording of the data subject's consent in instances where transactions are concluded telephonically or via electronic video feed.

8.5.9 Consent to process a data subject's personal information will be obtained directly from the data subject, except where:

- a) the personal information has been made public, or
- b) where valid consent has been given to a third party, or
- c) the information is necessary for effective law enforcement.

8.5.10 Employees and other persons acting on behalf of Spiddi Investments will under no circumstances:

- a) Process or have access to personal information where such processing or access is not a requirement to perform their respective work-related tasks or duties.
- b) Save copies of personal information directly to their own private computers, laptops or other mobile devices like tablets or smart phones. All personal information must be accessed and updated from Spiddi Investments central database or a dedicated server.
- c) Share personal information informally. Personal information should never be sent by email, as this form of communication is not secure. Where access to personal information is required, this may be requested from the relevant line manager or the Information Officer.
- d) Transfer personal information outside of South Africa without the express permission from the Information Officer.

8.5.11 Employees and other persons acting on behalf of Spiddi Investments are responsible for:

- a) Keeping all personal information that they meet secure, by taking sensible precautions and following the guidelines outlined within this policy.
- b) Ensuring that personal information is held in as few places as is necessary. No unnecessary additional records, filing systems and data sets should therefore be created.
- c) Ensuring that personal information is encrypted prior to sending or sharing the information electronically. The IT Manager will assist employees and where required, other persons acting on behalf of Spiddi Investments, with the sending or sharing of personal information to or with authorised external persons.
- d) Ensuring that all computers, laptops and devices such as tablets, flash drives and smartphones that store personal information are password protected and never left unattended. Passwords must be changed regularly and may not be shared with unauthorised persons.
- e) Ensuring that their computer screens and other devices are switched off or locked when not in use or when away from their desks.
- f) Ensuring that where personal information is stored on removable storage medias such as external drives, CDs or DVDs that these are kept locked away securely when not being used.

- g) Ensuring that where personal information is stored on paper, that such hard copy records are kept in a secure place where unauthorised people cannot access it. For instance, in a locked drawer of a filing cabinet.
- h) Ensuring that where personal information has been printed out, that the paper printouts are not left unattended where unauthorised individuals could see or copy them. For instance, close to the printer.
- i) Taking reasonable steps to ensure that personal information is kept accurate and up to date. For instance, confirming a data subject's contact details when the client or customer phones or communicates via email. Where a data subject's information is found to be out of date, authorisation must first be obtained from the relevant line manager or the Information Officer to update the information accordingly.
- j) Taking reasonable steps to ensure that personal information is stored only for as long as it is needed or required in terms of the purpose for which it was originally collected. Where personal information is no longer required, authorisation must first be obtained from the relevant line manager or the Information Officer to delete or dispose of the personal information in the appropriate manner.
- k) Undergoing POPI Awareness training from time to time.

8.5.12 Where an employee, or a person acting on behalf of Spiddi Investments, becomes aware or suspicious of any security breach such as the unauthorised access, interference, modification, destruction or the unsanctioned disclosure of personal information, he or she must immediately report this event or suspicion to the Information Officer or the Deputy Information Officer.

9. POPI AUDIT

9.1 Spiddi Investments Information Officer will schedule periodic POPI Audits.

The purpose of a POPI audit is to:

- a) Identify the processes used to collect, record, store, disseminate and destroy personal information.
- b) Determine the flow of personal information throughout Spiddi Investments. For instance, Spiddi Investments' various business units, divisions, branches and other associated organisations.

- c) Redefine the purpose for gathering and processing personal information.
- d) Ensure that the processing parameters are still adequately limited.
- e) Ensure that new data subjects are made aware of the processing of their personal information.
- f) Re-establish the rationale for any further processing where information is received via a third party.
- g) Verify the quality and security of personal information.
- h) Monitor the extend of compliance with POPIA and this policy.
- i) Monitor the effectiveness of internal controls established to manage Spiddi Investments's POPI related compliance risk.

9.2 In performing the POPI Audit, Information Officers will liaise with line managers to identify areas within in Spiddi Investments operation that are most vulnerable or susceptible to the unlawful processing of personal information.

9.3 Information Officers will be permitted direct access to and have demonstrable support from line managers and Spiddi Investment's governing body in performing their duties.

10. REQUEST TO ACCESS PERSONAL INFORMATION PROCEDURE

Data subjects have the right to:

- a) Request what personal information Spiddi Investments holds about them and why.
- b) Request access to their personal information.
- c) Be informed how to keep their personal information up to date.
- d) Access to information requests can be made by email, addressed to the Information Officer. The Information Officer will provide the data subject with a "Personal Information Request Form".



- e) Once the completed form has been received, the Information Officer will verify the identity of the data subject prior to handing over any personal information. All requests will be processed and considered against Spiddi Investments' PAIA Policy.
- f) The Information Officer will process all requests within a reasonable time.

11. POPI COMPLAINTS PROCEDURE

11.1 Data subjects have the right to complain in instances where any of their rights under POPIA have been infringed upon. Spiddi Investments takes all complaints very seriously and will address all POPI related complaints in accordance with the following procedure:

- a) POPI complaints must be submitted to Spiddi Investments in writing. Where so required, the Information Officer will provide the data subject with a "POPI Complaint Form".
- b) Where the complaint has been received by any person other than the Information Officer, that person will ensure that the full details of the complaint reach the Information Officer within 1 working day.
- c) The Information Officer will provide the complainant with a written acknowledgement of receipt of the complaint within 2 working days.
- d) The Information Officer will carefully consider the complaint and address the complainant's concerns in an amicable manner. In considering the complaint, the Information Officer will endeavour to resolve the complaint in a fair manner and in accordance with the principles outlined in POPIA.
- e) The Information Officer must also determine whether the complaint relates to an error or breach of confidentiality that has occurred, and which may have a wider impact on Spiddi Investments' data subjects.
- f) Where the Information Officer has reason to believe that the personal information of data subjects has been accessed or acquired by an unauthorised person, the Information Officer will consult with Spiddi Investments' governing body where after the affected data subjects and the Information Regulator will be informed of this breach.

- g) The Information Officer will revert to the complainant with a proposed solution with the option of escalating the complaint to Spiddi Investments' governing body within 7 working days of receipt of the complaint. In all instances, Spiddi Investments will provide reasons for any decisions taken and communicate any anticipated deviation from the specified timelines.
- h) The Information Officer's response to the data subject may comprise any of the following:
 - i. A suggested remedy for the complaint,
 - ii. A dismissal of the complaint and the reasons as to why it was dismissed,
 - iii. An apology (if applicable) and any disciplinary action that has been taken against any employees involved.
- i) Where the data subject is not satisfied with the Information Officer's suggested remedies, the data subject has the right to complain to the Information Regulator.
- j) The Information Officer will review the complaints process to assess the effectiveness of the procedure on a periodic basis and to improve the procedure where it is found wanting. The reason for any complaints will also be reviewed to ensure the avoidance of occurrences giving rise to POPI related complaints.

12. DISCIPLINARY ACTION

12.1 Where a POPI complaint or a POPI infringement investigation has been finalised, Spiddi Investments may recommend any appropriate administrative, legal and/or disciplinary action to be taken against any employee reasonably suspected of being implicated in any non-compliant activity outlined within this policy.

12.2 In the case of ignorance or minor negligence, Spiddi Investments will undertake to provide further awareness training to the employee.

12.3 Any gross negligence or the wilful mismanagement of personal information will be considered a serious form of misconduct for which Spiddi Investments may summarily dismiss the employee. Disciplinary procedures will commence where there is sufficient evidence to support an employee's gross negligence.

12.4 Examples of immediate actions that may be taken after an investigation include:



- a) A recommendation to commence with disciplinary action.
- b) A referral to appropriate law enforcement agencies for criminal investigation.
- c) Recovery of funds and assets to limit any prejudice or damages caused.

ANNEXURE A: EMPLOYEE CONSENT AND CONFIDENTIALITY CLAUSE

EMPLOYEE CONSENT AND CONFIDENTIALITY CLAUSE

- "Personal Information" (PI) shall mean the race, gender, sex, pregnancy, marital status, national or ethnic origin, colour, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language and birth of a person; information relating to the education or the medical, financial, criminal or employment history of the person; any identifying number, symbol, email 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 whether the information is recorded electronically or otherwise.
- "POPIA" shall mean the Protection of Personal Information Act 4 of 2013 as amended from time to time.
- The employer undertakes to process the PI of the employee only in accordance with the conditions of lawful processing as set out in terms of POPIA and in terms of the employer's relevant policy available to the employee on request and only to the extent that it is necessary to discharge its obligations and to perform its functions as an employer and within the framework of the employment relationship and as required by South African law.

- The employee acknowledges that the collection of his/her PI is both necessary and requisite as a legal obligation, which falls within the scope of execution of the legal functions and obligations of the employer. The employee therefore irrevocably and unconditionally agrees:
 - That he/she is notified of the purpose and reason for the collection and processing of his or her PI insofar as it relates to the employer's discharge of its obligations and to perform its functions as an employer.
 - That he/she consents and authorises the employer to undertake the collection, processing and further processing of the employee's PI by the employer for the purposes of securing and further facilitating the employee's employment with the employer.
 - Without derogating from the generality of the afforested, the employee consents to the employer's collection and processing of PI pursuant to any of the employer's Internet, Email and Interception policies in place insofar as PI of the employee is contained in relevant electronic communications.
 - To make available to the employer all necessary PI required by the employer for the purpose of securing and further facilitating the employee's employment with the employer.
 - To absolve the employer from any liability in terms of POPIA for failing to obtain the employee's consent or to notify the employee of the reason for the processing of any of the employee's PI.
 - To the disclosure of his/her PI by the employer to any third party, where the employer has a legal or contractual duty to disclose such PI.
 - The employee further agrees to the disclosure of his/her PI for any reason enabling the employer to carry out or to comply with any business obligation the employer may have or to pursue a legitimate interest of the employer in order for the employer to perform its business on a day-to-day basis.
 - The employee authorises the employer to transfer his/her PI outside of the Republic of South Africa for any legitimate business purpose of the employer within the international community. The employer undertakes not to transfer or disclose his/her PI unless it is required for its legitimate business requirements and shall comply strictly with legislative stipulations in this regard.
- The employee acknowledges that during the performance of his/her services, he/she may gain access to and become acquainted with the personal information of certain clients, suppliers and other employees. The employee will treat personal information as a confidential business asset and agrees to respect the privacy of clients, suppliers and other employees.

- To the extent that he/she is exposed to or insofar as PI of other employees or third parties are disclosed to him/her, the employee hereby agrees to be bound by appropriate and legally binding confidentiality and non-usage obligations in relation to the PI of third parties or employees.
- Employees may not directly or indirectly, utilise, disclose or make public in any manner to any person or third party, either within the organisation or externally, any personal information, unless such information is already publicly known or the disclosure is necessary for the employee or person to perform his or her duties on behalf of the employer.

ANNEXURE B: SLA CONFIDENTIALITY CLAUSE

SLA CONFIDENTIALITY CLAUSE

- “Personal Information” (PI) shall mean the race, gender, sex, pregnancy, marital status, national or ethnic origin, colour, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language and birth of a person; information relating to the education or the medical, financial, criminal or employment history of the person; any identifying number, symbol, email 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 whether the information is recorded electronically or otherwise.

- “POPIA” shall mean the Protection of Personal Information Act 4 of 2013 as amended from time to time.
- The parties acknowledge that for the purposes of this agreement that the parties may come into contact with, or have access to PI and other information that may be classified, or deemed as private or confidential and for which the other party is responsible. Such PI may also be deemed or considered as private and confidential as it relates to any third party who may be directly or indirectly associated with this agreement. Further, it is acknowledged and agreed by the parties that they have the necessary consent to share or disclose the PI and that the information may have value.
- The parties agree that they will at all times comply with POPIA’s Regulations and Codes of Conduct and that it shall only collect, use and process PI it comes into contact with pursuant to this agreement in a lawful manner, and only to the extent required to execute the services, or to provide the goods and to perform their respective obligations in terms of this agreement.
- The parties agree that it shall put in place, and always maintain, appropriate physical, technological and contractual security measures to ensure the protection and confidentiality of PI that it, or its employees, its contractors or other authorised individuals meets pursuant to this agreement.
- Unless so required by law, the parties agree that it shall not disclose any PI as defined in POPIA to any third party without the prior written consent of the other party, and notwithstanding anything to the contrary contained herein, shall any party in no manner whatsoever transfer any PI out of the Republic of South Africa.

