Policy Statement, Manual and Code of Conduct

for

Lester Hall Fletcher Inc.

(herein after referred to as "the firm")

in respect of the Protection of Personal Information Act 2013

(POPIA)

This document does not replace the relevant provisions in POPIA but operates in support of the requirements in POPIA. A code cannot limit a data subject's right to privacy, which can only be done as provided for in POPIA.

The commencement date of POPIA

Parliament assented to POPIA on 19 November 2013. The commencement date of section 1, Part A of Chapter 5, section 112 and section 113 is 11 April 2014. The commencement date of the other sections is 1 July 2020 (with the exception of section 110 and 114(4). The President of South Africa has proclaimed the POPI commencement date to be 1 July 2020.

Latest update: 13 May 2021

TABLE OF CONTENTS

1 INTRODUCTION 3

2 DEFINITIONS 3

3 POLICY PURPOSE 6

4 POLICY APPLICATION 7

5 RIGHTS OF DATA SUBJECTS 7

6 GENERAL GUIDING PRINCIPLES 8

7 INFORMATION OFFICERS 11

8 SPECIFIC DUTIES AND RESPONSIBILITIES 12

9 POPI AUDIT 16

10 REQUEST TO ACCESS PERSONAL INFORMATION PROCEDURE 16

11 POPI COMPLAINTS PROCEDURE 17

12 DISCIPLINARY ACTION 18

13 INFORMATION SECURITY MANAGEMENT SYSTEM 18

14 DATA BREACH PROTOCOL 23

14.1 The Firm shall notify the affected Data Subject in writing immediately or otherwise as soon as reasonably possible, if any Personal Information under the control of the Firms as a result of the Agreement and/or mandate between the Data Subject and the firm has been or may reasonably believe to have been accessed or acquired by an unauthorised person or if a breach has occurred with reference to the Firm's use of the Personal Information under the Agreement and/or mandate. 23

14.2 The Firm shall furnish the Data Subject with details of the Data Subjects affected by the compromise and the nature and extent of the compromise, including details of the identity of the unauthorised person who may have accessed or acquired the Personal Information as well as with daily reports on progress made at resolving the compromise; within 3 (three) Business Days of receipt thereof, of any request for access to or correction of the Personal Information or complaints received by the firm relating to its obligations in terms of POPI and provide data subjects with full details of such request or complaint; and Promptly of any legally binding request for disclosure of Personal Information or any other notice or communication that relates to the Processing of the Personal Information from any supervisory or governmental body. The Firm acknowledges and agrees that the Data Subject retains all right, title and interest in and to the Personal Information and that the Personal Information shall constitute the Data Subject's Confidential Information. 23

15 INDUCTION 24

16 UPDATE OF POLICY 24

1 INTRODUCTION

The ability to process increasingly large volumes of information in respect of individuals are one of the major threats that the information revolution holds to our society. The right to privacy is an integral human right recognised and protected in the South African Constitution. The Protection of Personal Information Act 4 of 2013 (hereinafter referred to as "POPIA") provides the framework for the enforcement of the right to privacy. The purpose of POPIA is, amongst others to establish safeguards for the confidentiality and integrity of personal information and more importantly to give effect to the constitutional right to privacy by safeguarding personal information when processed by a responsible party. POPIA applies to the processing of personal information entered in a record by or for a responsible party by making use of automated or non-automated means provided that when the recorded personal information is processed by non-automated means, it forms part of a filing system or is intended to form part thereof; and where the responsible party is domiciled in the Republic or not domiciled in the Republic but makes use of automated and non-automated means in the Republic unless those means are used only to forward personal information through the Republic.

The stipulations of POPIA correspond directly to our professional obligation to maintain the confidentiality and integrity of information processed in electronic form in respect of our clients, employees, and all other data subjects.

Our dependence on information and communication technologies has brought risks with it. In order to protect all data subjects from harm, the firm is committed to effectively manage, regulate and protect personal information according to the provisions of POPIA. This policy and manual confines itself to the issue of risk to personal information and the duties of our firm in respect thereof.

The threat to privacy adversely affects our practise unless we comply with our professional and statutory duties. We have always dealt with paper and text and have developed appropriate safeguards to the protection of confidentiality and integrity. These safeguards will still apply as POPIA is not confined to electronic information but covers information in paper and text as well.

Chapter 3 of POPIA regulates the processing of personal information by or for a responsible party through compliance with the eight (8) conditions for the lawful processing of personal information, the processing of special personal information and the processing of personal information of children.

2 DEFINITIONS

2.1 **Personal Information**

Personal information relates to any information that reveal the identity of a person. Personal Information is described in POPIA as an identifiable, living, natural person, and where applicable, an identifiable, existing juristic person and include but is not limited to, information relating to, inter alia

2.1.1 the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;

2.1.2 information relating to the education or the medical, financial, criminal or employment history of the person; any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person; the biometric information of the person;

2.1.3 the personal opinions, views or preferences of the person;

2.1.4 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;

2.1.5 the views or opinions of another individual about the person; and

2.1.6 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 for instance an employee of the firm, a client, and adversary in litigation, a witness in litigation or a seller and purchaser in conveyancing and/or a supplier to the firm.

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. The firm 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 instance, a third-party IT service provider that has contracted with the firm.

2.5 **Information Officer**

The Information Officer is responsible for ensuring the firm's compliance with POPIA. Where no Information Officer is appointed, the managing director of the firm will be responsible for performing the Information Officer's duties. 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 includes any activity or any set of operations, whether or not by automatic means, concerning personal information, including;

2.6.1 the collection, receipt, recording, firm, storage, updating or modification, retrieval, alteration, consultation or use;

2.6.2 dissemination by means of transmission, distribution or making available in any other form;

2.6.3 or merging, linking, as well as any restriction, degradation, deletion or destruction of information.

2.7 **Record**

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

2.7.1 Writing on any material;

2.7.2 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;

2.7.3 Label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;

2.7.4 Book, map, plan, graph or drawing;

2.7.5 Photograph, film, negative, tape or other device in which one or more visual images are embodied 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 promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject or requesting the data subject to make a donation of 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

This purpose of this policy is to protect the firm from the compliance risks associated with the protection of personal information which include a breach of confidentiality, failing to offer choice and reputational damage which in turn, can cause the firm to suffer loss in revenue where it is found that the personal information of data subjects has been shared or disclosed inappropriately. All data subjects should be free to choose how and for what purpose the firm uses information relating to them. In terms of Section 11 of POPIA information may only be processed if the data subject or a competent person, where the data subject is a child, consents to the processing, the processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party, processing complies with an obligation imposed by law on the responsible party, processing protects a legitimate interest of the data subject, processing is necessary for the proper performance of a public law duty by a public body or processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied.

This policy demonstrates the firm's commitment to protecting the privacy rights of data subjects through stating desired behaviour and directing compliance with the provisions of POPIA. The firm hereby declare to cultivate a culture that recognises privacy as a valuable human rights and to develop and implement internal controls for the purpose of managing the compliance risk associated with the protection of personal information. This policy shall further aim to implement business practices that will provide reasonable assurance that the rights of data subjects are protected and balanced with the operational needs of the firm. Specific duties and responsibilities shall be assigned to control personal, including the appointment of an Information Officer and where necessary, Deputy Information Officers in order to protect the interests of the firm and data subjects. The firm further aims to raise awareness through training and providing guidance to all employees who process personal information to enable them to act confidently and consistently.

4 POLICY APPLICATION

This policy and its guiding principles apply to all departments in the law firm. It further applies to all employees, temporary employees, volunteers, all contractors, suppliers, and other persons acting on behalf or in the interest of the firm. The policy's guiding principles find application in all situations and must be read in conjunction with POPIA as well as the Promotion of Access to Information Act (Act No 2 of 2000). The legal duty to comply with POPIA's provisions is activated in any situation where there is processing of personal information entered into a record by or for a responsible person who is domiciled in South Africa.

5 RIGHTS OF DATA SUBJECTS

Where appropriate, the firm will ensure that its clients are made aware of the rights conferred upon them as data subjects. The firm will ensure that it gives effect to the following seven rights contained in POPIA.

5.1 **The Right to Access Personal Information**

The firm recognises that a data subject has the right to establish whether the firm holds personal information related to him, her or it, including the right to request access to that personal information. An example of a "Personal Information Request Form" can be found under **Annexure "PA"**.

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 the firm is no longer authorised to retain the personal information.

5.3 **The Right to Object to the Processing of Personal Information**

The data subject has the right, on reasonable grounds, to object to the processing of his, her or its personal information. In such circumstances, the firm will give due consideration to the request, the operational needs of the firm and the requirements of POPIA.

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.

5.6 **The Right to be Informed**

The data subject has the right to be notified that his, her or its personal information is being collected by the firm. The data subject also has the right to be notified in any situation where the firm 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

Directors and all other employees acting on behalf of the firm will at all times be subject to, and act in accordance with, the following guiding principles:

6.1 **Accountability**

Failing to comply with POPIA could potentially damage the firm's reputation or expose the firm to a civil claim for damages. The protection of personal information is therefore the responsibility of each director, associate, candidate attorney, para-legal and all or any support staff. The representatives shall always ensure that the provisions of POPIA and the guiding principles outlined in this policy are complied with. The firm 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**

The firm shall ensure that personal information under its control is processed in a fair, lawful and non-excessive manner, on with the informed consent of the data subject, and only for a specifically defined purpose. The firm shall inform the data subject of the reasons for collecting his, her or its personal information and obtain written consent prior to processing personal information should same not be collected as a result of taking actions for the conclusion or performance of a contract to which the data subject is party, processing complies with an obligation imposed by law on the responsible party, processing protects a legitimate interest of the data subject or processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied. Alternatively, where services or transactions are concluded over the telephone or electronic video feed and/or electronic mail, the firm shall maintain a printed copy of the electronic mail which shall state and confirm the purpose for collecting the personal information. The firm shall under no circumstances distribute or share personal information between separate legal entities, associated firms or with any individuals that are not directly involved with facilitating the purpose for which the information was originally collected. An example of a "POPIA Notice and Consent Form" can be found under **Annexure "PB"**.

6.3 **Purpose Specification**

The firm shall process personal information only for specific, explicitly defined and legitimate reasons and which only form part and is partial to the execution of any instruction and or mandate received by the specific client or clients. The firm shall inform data subjects of these reasons prior to collecting or recording the data subject's personal information. The Purpose specification must be outlined in the Consent Form.

6.4 **Further Processing Limitation**

Personal information shall not be processed for a secondary purpose unless that

processing is compatible with the original purpose. Therefore, where the firm 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, the firm will first obtain additional consent from the data subject.

6.5 **Information Quality**

The firm shall take reasonable steps to ensure that all personal information collected is complete, accurate and not misleading. Where personal information is collected or received from third parties, the firm shall take reasonable steps to confirm that the information is correct by verifying the accuracy of the information directly with the data subject.

6.6 **Open Communication**

The firm shall take reasonable steps to ensure that data subjects are at all times aware that their personal information is being collected, including the purpose for which it is being collected and processed. The firm shall ensure that it establishes and maintains proper communication with the data subjects. Our firm has an existing website and Facebook account which provides all necessary contact detail, should a data subject want to enquire whether the firm holds related personal information, request access to related personal information or request the firm to update or correct personal information, or lodge a complaint concerning the processing of their personal information.

6.7 **Security Safeguards**

The firm will manage the security of its filing system to ensure that personal information is adequately protected. To this end, security controls will be implemented in order to minimise the risk of loss, unauthorised access, disclosure, interference, modification, or destruction. The firm shall continuously review its security controls which will include regular testing of protocols and measures put in place to combat cyber-attacks on the firm's IT network. The firm will ensure that all paper and electronic records comprising personal information are securely stored and made accessible only to authorised individuals. 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 the firm is responsible. All existing employees will, after the required consultation and training process, be required to sign an addendum to their employment contract containing the relevant consent and confidentiality clauses. The operators of the firm and third-party service providers will be required to enter into service level agreements with the firm where both parties pledge their mutual commitment to POPIA and the lawful processing of any personal information pursuant to the agreement.

6.8 **Data Subject Participation**

A data subject may request the correction or deletion of his, her or its personal information held by the firm. The firm will ensure that it provides a facility for data subjects who want to request the correction of deletion of their personal information.

7 INFORMATION OFFICERS

To enable the firm as a responsible party to exercise the control over personal information required by the Accountability Condition contained in the Act, two critical control measures need to be established and maintained:

- The personal information being processed by a responsible party needs to be identified; and

- The responsible party must identify and appoint a person (or persons) charged with the safeguarding of personal information.

With regard to the latter of the two control measures, the Act provides for the appointment of an Information Offices. In the case of a private body such as our firm, an Information Officer means the head of the private body as contemplated in Section 1 of PAIA. In this instance the duties of the Information Officer may be delegated by the head of the private body.

The firm shall from time to time appoint an Information Officer and where necessary, a Deputy Information Officer to assist the Information Officer. The firm's Information Officer is responsible for ensuring compliance with POPIA. There are no legal requirements under POPIA for the firm to appoint an Information Officer. Appointing an Information Officer is however, considered to be a good business practice, particularly within larger firms. Where no Information Officer is appointed, the managing director of the firm will assume the role of the Information Officer. Consideration will be given on an annual basis to the re-appointment or replacement of the Information Officer and the reappointment or replacement of any Deputy Information Officers. Once appointed, the firm will register the Information Officer with the South African Information Regulator established under POPIA prior to performing his or her duties.

Information Officer Duly Appointed:

Wendy De Bruyn

Attorney and Conveyancer

Email: wendy@lesterhall.co.za

TEL: 0861 2777 27

Deputy Information Officer Duly Appointed:

Daniyle Mallon

Office Manager

Email: daniyle@lesterhall.co.za

TEL: 0861 2777 27

8 SPECIFIC DUTIES AND RESPONSIBILITIES

8.1 Governing Body

The firm's governing body cannot delegate its accountability and is ultimately answerable for ensuring that the firm meets its legal obligations in terms of POPIA. The governing body may however delegate some of its responsibilities in terms of POPIA to management or other capable individuals.

The governing body is responsible for ensuring that:

8.1.1 The firm appoints an Information Officer;

8.1.2 All persons responsible for the processing of personal information on behalf of the firm are *inter alia*, appropriately trained to do so, understand that they are contractually obligated to protect the personal information they come into contact with, and are aware that a wilful or negligent breach of this policy's processes and procedures may lead to disciplinary action being taken against them.

8.1.3 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.

8.1.4 The scheduling of a periodic POPI Audit in order to accurately assess and review the ways in which the firm collects, holds, uses, shares, discloses, destroys and processes personal information.

8.2 Information Officer

The firm's Information Officer is responsible for:

8.2.1 Taking steps to ensure the firm's reasonable compliance with the provision of POPIA.

8.2.2 Attend any seminar or workshop held by the regulator to ensure the firm's

continue compliance with POPIA.

8.2.3 Continually analysing privacy regulations and aligning them with the firm's personal information processing procedures

8.2.4 Ensuring that POPI Audits are scheduled and conducted on a regular basis.

8.2.5 Ensuring that the firm makes it convenient for data subjects who want to update their personal information or submit POPI related complaints to the firm.

8.2.6 Approving any contracts entered into with operators, employees and other third parties which may have an impact on the personal information held by the firm. This will include overseeing the amendment of the firm's employment contracts and other service level agreements.

8.2.7 Encouraging compliance with the conditions required for the lawful processing of personal information.

8.2.8 Ensuring that employees and other persons acting on behalf of the firm are fully aware of the risks associated with the processing of personal information and that they remain informed about the firm's security controls.

8.2.9 Organising and overseeing the awareness training of employees and other individuals involved in the processing of personal information on behalf of the firm.

8.2.10 Addressing employees' POPIA related questions.

8.2.11 Addressing all POPIA related requests and complaints made by the firm's data subjects.

8.2.12 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, with regard to any other matter. The Deputy Information Officer will assist the Information Officer in performing his or her duties.

8.3 **Employees and all other Persons acting on behalf and/or representing the firm**

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

persons acting on behalf of the firm are required to treat personal information as a confidential business asset and to respect the privacy of data subjects. Employees and other persons acting on behalf of the firm may not directly or indirectly, utilise, disclose or make public in any manner to any person or third party, either within the firm 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. Employees and other persons acting on behalf of the firm 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. Employees and other persons acting on behalf of the firm will;

8.3.1 Only process personal information where the data subject, or a competent person where the data subject is a child, consents to the processing; or

8.3.2 Only process personal information where 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

8.3.3 Only process personal information where the processing complies with an obligation imposed by law on the responsible party; or

8.3.4 Only process personal information where the processing protects a legitimate interest of the data subject; or

8.3.5 Only process personal information where the processing is necessary for pursuing the legitimate interests of the firm or of a third party to whom the information is supplied

8.3.6 Personal information will only be processed where the data subject clearly understands why and for what purpose his, her or its personal information is being collected; and has granted the firm with explicit written or verbally recorded consent to process his, her or its personal information and keeping all personal information that they come into contact with secure, by taking sensible precautions and following the guidelines outlined within this policy.

8.3.7 Employees and other persons acting on behalf of the firm 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. 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. Consent can be obtained in written form which includes any appropriate electronic medium that is

accurately and readily reducible to printed form. Alternatively, the firm will keep a voice recording of the data subject's consent in instances where transactions are concluded telephonically or via electronic video feed.

8.3.8 Ensure 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. and ensure 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

8.3.9 Ensure 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.

8.3.10 Ensure that where personal information has been printed out, that the paper printouts are not left unattended where unauthorised individuals could see or copy them.

8.3.11 Take reasonable steps to ensure that personal information is kept accurate and up to date. 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.

8.3.12 Take 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.

8.3.13 Undergoing POPI Awareness training from time to time.

8.3.14 Where an employee, or a person acting on behalf of the firm, 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.

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

8.3.15.1 the personal information has been made public, or

8.3.15.2 where valid consent has been given to a third party, or

8.3.15.3 the information is necessary for effective law enforcement.

8.3.16 Employees and other persons acting on behalf of the firm will under no circumstances:

8.3.16.1 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.

8.3.16.2 Save copies of personal information directly to their own private computers, laptops or other mobile devices like tablets or smart phones.

8.3.16.3 Transfer personal information outside of South Africa without the express permission from the Information Officer.

9 POPI AUDIT

The firm's Information Officer will schedule periodic POPI Audits. The purpose of a POPI audit are to:

9.1 Identify the processes used to collect, record, store, disseminate and destroy personal information.

9.2 Determine the flow of personal information throughout the firm.

9.3 Redefine the purpose for gathering and processing personal information. Ensure that the processing parameters are still adequately limited.

9.4 Ensure that new data subjects are made aware of the processing of their personal information.

9.5 Verify the quality and security of personal information.

9.6 Monitor the extend of compliance with POPIA and this policy.

9.7 Monitor the effectiveness of internal controls established to manage the firm's POPIA related compliance risk. In performing the POPI Audit, Information Officers will liaise with line managers in order to identify areas within in the firm's operation that are most vulnerable or susceptible to the unlawful processing of personal information. Information

10 REQUEST TO ACCESS PERSONAL INFORMATION PROCEDURE

Data subjects have the right to:

10.1 Request what personal information the firm holds about them and why.

10.2 Request access to their personal information.

10.3 Be informed how to keep their personal information up to date. 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”. 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 the firm’s PAIA Policy. The Information Officer will process all requests within a reasonable time.

11 POPI COMPLAINTS PROCEDURE

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

11.1 POPIA complaints must be submitted to the firm in writing. Where so required, the Information Officer will provide the data subject with a “POPI Complaint Form” to be drafted by the Information Officer.

11.2 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 reaches Information Officer within 2 working days.

11.3 The Information Officer will provide the complainant with a written acknowledgement of receipt of the complaint within 2 working days.

11.4 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.

11.5 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 the firm’s data subjects.

11.6 Where the Information Officer has reason to believe that the personal information of data subjects have been accessed or acquired by an unauthorised person, the Information Officer will consult with the firm’s governing body where after the affected data subjects and the Information Regulator will be informed of this breach.

11.7 The Information Officer will revert to the complainant with a proposed solution with the option of escalating the complaint to the firm's governing body within 7 working days of receipt of the complaint. In all instances, the firm will provide reasons for any decisions taken and communicate any anticipated deviation from the specified timelines.

11.8 The Information Officer's response to the data subject may suggest a remedy for the complaint, a dismissal of the complaint and the reasons as to why it was dismissed, an apology (if applicable) and any disciplinary action that has been taken against any employees involved.

11.9 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.

11.10 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

Where a POPI complaint or a POPI infringement investigation has been finalised, the firm 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. In the case of ignorance or minor negligence, the firm will undertake to provide further awareness training to the employee. Any gross negligence or the wilful mismanagement of personal information, will be considered a serious form of misconduct for which the firm may summarily dismiss the employee. Disciplinary procedures will commence where there is sufficient evidence to support an employee's gross negligence.

13 INFORMATION SECURITY MANAGEMENT SYSTEM

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

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

13.1 The information officer is Wendy De Bruyn whose details are available at paragraph 7 herein and who is responsible for compliance with the conditions of the lawful processing of personal information and other provisions of POPIA;

13.2 This Policy has been put in place throughout the firm, which include the litigation, conveyancing, accounting and general administration departments and training on this

policy and the POPIA Act have already taken place and will take place during 2021/22.

13.3 The firm has done a risk assessment to determine where the risk to our clients and lie.

13.4 We have identified the relevant role players and appointed the correct people to safeguard all personal information, we have mapped our activities, recorded how to process data lawfully and have implemented the correct action items.

13.5 We have identified quick successes and have implemented the following:

13.5.1 **Information Classification.**

A framework describing how information must be classified within the practice has been established:

- *Confidential Information***.** Access to this information must only be granted to persons authorised by the owner of the information;
- *Restricted Information*. All employees of the practice are authorised to have access to the information. Third parties engaged by the practice and who are subject to an information security agreement may have access to the information;
- *Public Information.* This information is information which, through a mechanism of approval, has been declared to be public information by the practice.

In the normal course a proper classification would find that the vast majority of the information processed within an attorney's practice such as our firm (at least 90%) would be "restricted". This information should nonetheless, by the nature of attorney's practices and their confidentiality obligations, still be strictly controlled to ensure the preservation of confidentiality and, where appropriate, attorney and client privilege.

13.5.2 **Human Resources Security**

The firm must ensure that persons dealing with information understand their responsibilities, are suitable to the roles that they may be considered for and that their security responsibilities are addressed prior to employment in terms of appropriate agreements. All employees must understand their information security responsibilities. This will in the normal course be achieved by documenting information security responsibilities in employment contracts and in Acceptable Use Policies which must be accepted by the employee prior to

being granted access to the practice's information systems or its information.

We have identified the framework in respect of Human Resource Security as the following;

Prior to engagement the firm shall screen employees and third parties who may be granted access to sensitive information.

During their engagement employees shall be subject to information security policies, must receive appropriate awareness, education and training and breaches should be subject to disciplinary procedures. Third parties should be subject to proportionate arrangements contained in third party agreements. Changes of engagement must be subject to proper change control mechanisms which revoke employees rights to information which they will no longer require in the course of their engagement and formally authorise and grant access to information that the new engagement requires.

On termination of engagement controls shall be in place to remove access privileges to physical premises, the revocation of rights of access to information and the return or destruction of information in the possession of the person whose engagement is terminated. Particularly as electronic technologies have made vast amounts of information extremely portable, the barriers which previously existed to the removal of information on paper have disappeared. It is therefore critical that appropriate exit policies and procedures are formulated and properly implemented.

13.5.3 **Governance and Management of Information Processing and Communications Facilities**

The management of our information system is in the hands of third parties. We rely on technology vendors and technology support companies to manage our information systems. The objective of control measures relating to communications and operations management are to ensure that the information processing facilities of the practice operate correctly and securely. To the extent that responsibilities are delegated to third parties there should be written agreements which record and govern the third party's obligations. The following responsibilities of the third party will provide some guidance as to important issues to be addressed in agreements with third parties.

- Operating procedures shall support the firm's information security policies;
- Operating procedures must be properly documented;

- Changes to technologies facilitating information processing and communication must be made with due care for the security of information and avoidance of disruptions to the practice;

- Access to information systems and information must only be granted against appropriate authority of the owners of the information systems and/or information;

- The development and acquisition of all new technologies must take into consideration and ensure information security capability in the developed or newly acquired technologies;

- Information and communications technologies must be tested prior to implementation in the operational environment to avoid unnecessary disruption;

- Protections against malicious and mobile code (viruses) must be implemented;

- Appropriate backup of information and information systems must be implemented;

- Records, including but not limited to audit trails and logs of usage of information must be retained;

- All media on which the practice's information may be stored (particularly where removed from the physical protection afforded by the practice) must be appropriately controlled;

- Where computer equipment is to be disposed of or destroyed the information must either be removed from the equipment or destroyed in a manner that it cannot be reconstructed;

- Generally best practice supporting the establishment and maintenance of information security must be applied.

- The information officer and deputy information officer to work closely with the service provider, regularly review the service provision and ensure that the services are being provided in terms of the agreement and information security principles inherent in that agreement.

- The Information Officer will also facilitate the planning of changes to systems, upgrading of systems and implementation of third party systems

which may need to integrate with existing systems.

- The Information Officer and Directors must monitor communications with third parties (not the content of the communications but the communications traffic). Persons responsible for the administration of communication systems should ensure that proper logs of communications are retained, a monitoring system used to ensure that capacity is adequate, faults and the rectification thereof are logged, adequate backup is available at all times, in the event of system failures these can be rectified with the least possible disruption and generally administering the information system in line with good practice and generally accepted information security

- Cryptographic controls are being used to protect the confidentiality, authenticity and integrity of information.

- More sophisticated control mechanisms such as the use of digital certificates have been implemented to authenticate identity.

13.5.4 **Access Control to Information and Compliance**

The objective is to control access to information and to avoid breaches of any law, statutory, regulatory or contractual obligation and breaches of any security requirements.

- The firm established mechanisms to authenticate the user such as the control of passwords, where passwords we ensure that strong passwords are created and established through well-formulated and implemented password policies, procedures and standards.

- unattended equipment must be controlled to prevent unauthorised access and “clear desk” and “clear screen” policies have been implemented.

- Awareness Training and risk assessment.

- We have 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 the use and storage of employee information, or any other action so required, in terms of POPIA.

- Every employee currently employed within the firm 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.

- All files will be archived at the Firm's disaster recovery site which will be available in case of a breach.

- A Security Incident Management Register will be kept to log any security incidents and to report on and manage said incidents this register will be maintained by the appointed Information Officer.

- Consent to process debtor information is obtained from clients (or a person who has been given authorisation from the client to provide the client's Personal Information) during the introductory, appointment and need analysis stage of the relationship.

14 DATA BREACH PROTOCOL

14.1 The Firm shall notify the affected Data Subject in writing immediately or otherwise as soon as reasonably possible, if any Personal Information under the control of the Firms as a result of the Agreement and/or mandate between the Data Subject and the firm has been or may reasonably believe to have been accessed or acquired by an unauthorised person or if a breach has occurred with reference to the Firm's use of the Personal Information under the Agreement and/or mandate.

14.2 The Firm shall furnish the Data Subject with details of the Data Subjects affected by the compromise and the nature and extent of the compromise, including details of the identity of the unauthorised person who may have accessed or acquired the Personal Information as well as with daily reports on progress made at resolving the compromise; within 3 (three) Business Days of receipt thereof, of any request for access to or correction of the Personal Information or complaints received by the firm relating to its obligations in terms of POPI and provide data subjects with full details of such request or complaint; and Promptly of any legally binding request for disclosure of Personal Information or any other notice or communication that relates to the Processing of the Personal Information from any supervisory or governmental body. The Firm acknowledges and agrees that the Data Subject retains all right, title and interest in and to the Personal Information and that the Personal Information shall constitute the Data Subject's Confidential Information.

15 INDUCTION

The documentation for staff is contained in this policy document and other materials made available by the Information Officer.

15.1 The firm's 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.

15.2 Continuing training will provide opportunities for staff to explore POPIA Act issues through training, team meetings, and supervisions.

15.3 The firm must ensure that all staff sign acceptance of this policy once they have had the opportunity to understand the policy and their responsibilities in terms of the policy and the POPIA Act.

16 UPDATE OF POLICY

This policy shall be updated when the Regulator provides updated regulations or recommendations, or the governing body deem it necessary. Further, the policy shall be the legal framework for compliance with POPIA within our firm and a copy of same shall be held in the office of the Information Officer.