



# **PROTECTION OF PERSONAL INFORMATION ("POPI") POLICY**

**ERASMUS-ELS INCORPORATED  
(TRADING AS ERASMUS-SCHEEPERS ATTORNEYS)**

<b>Document Ref.</b>	POPI-2
<b>Version:</b>	1.0
<b>Dated:</b>	23 July 2021

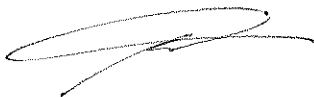
## Revision History

Version	Date	Revision Author	Summary of Changes

## Distribution

Name	Title
CAF Morkel	Director/Deputy Information Officer
DJ de Waal	Director/Deputy Information Officer
All employees	

## Approval

Name	Position	Signature	Date
MC Erasmus	Managing Director/Information Officer		23 July 2021

## TABLE OF CONTENTS:

No.	Clause	Pages
1.	DEFINITIONS	4
2.	INTRODUCTION	7
3.	PURPOSE	7
4.	APPLICABILITY	8
5.	INFORMATION OFFICER AND DEPUTY INFORMATION OFFICER	9
6.	DE-IDENTIFYING PERSONAL INFORMATION	9
7.	RIGHTS OF DATA SUBJECTS	10
8.	REQUIREMENTS FOR LAWFUL PROCESSING	12
9.	ACCESS AND SECURITY TO INFORMATION/RECORDS	20
10.	TECHNICAL AND ORGANISATIONAL MEASURES	20
11.	PERFORMING A POPI GAP ANALYSIS AND RISK ASSESSMENTS	23
12.	POPI AND E-MAIL USAGE	24
13.	COMPLIANCE MANAGEMENT FRAMEWORK	26
14.	PROCESSING OF INFORMATION BY USING AUTOMATED AND NON-AUTOMATED MEANS	26
15.	SPECIFIC DUTIES AND RESPONSIBILITIES	26
16.	REQUEST TO ACCESS PERSONAL INFORMATION PROCEDURE	35
17.	FORBIDDEN USES OF DATA SUBJECT'S PERSONAL INFORMATION	36
18.	COMPANY'S RIGHT TO ACCESS INFORMATION	37
19.	BREACH OF SECURITY/ UNAUTHORISED ACCESS TO INFORMATION	38
20.	CORPORATE POLICY GUIDELINE	38
21.	MONITORING AND IMPLEMENTATION OF THE POLICY	39
22.	POPI COMPLAINTS PROCEDURE	40
23.	DISCIPLINARY ACTION	40

## 1. DEFINITIONS

In this Policy, unless the context indicates a contrary intention, the following words and expressions bear the meanings assigned to them and cognate expressions bear corresponding meanings:

- 1.1. **"Act"** means the Protection of Personal Information Act, Act No. 4 of 2013 (as amended);
- 1.2. **"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;
- 1.3. **"Client"** means any person who engages the services of the Company;
- 1.4. **"Company"** means Erasmus-Els Incorporated, trading as Erasmus-Scheepers Attorneys, a personal liability company, duly incorporated in terms of the Companies Act, 2008, with registration number 2002/015175/21 as well as any of its current or future associated brands or entities;
- 1.5. **"Compliance Framework"** means the Compliance Management Framework adopted by the Company to ensure that the necessary steps are taken to comply with POPI;
- 1.6. **"Consent"** means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of Personal Information;
- 1.7. **"Data Subject"** refers to the natural or juristic person to whom Personal Information relates, such as an individual client, customer or a company that supplies the organisation with products or other goods.
- 1.8. **"De-Identify"** 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;
- 1.9. **"Direct Marketing"** means to approach a Data Subject, either in person or by mail or electronic communication, for the direct or indirect purpose of:
  - 1.9.1. Promoting or offering to supply, in the ordinary course of business, any goods or services to the Data Subject; or
  - 1.9.2. Requesting the Data Subject to make a donation of any kind for any reason.

- 1.10. **"Directors"** means the directors serving on the Board of Directors of the Company, from time to time;
- 1.11. **"Employee/s/"** means any person who works for the Company and who receives, or is entitled to receive, any remuneration, and any other person who in any manner assists in carrying on or conducting the business of the Company;
- 1.12. **"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;
- 1.13. **"Information Officer"** means the designated compliance officer appointed by the Company to address compliance with the Act, from time to time;
- 1.14. **"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;
- 1.15. **"PAIA"** means the Promotion of Access to Information Act, 2 of 2000;
- 1.16. **"Personal Information"** shall have the meaning assigned to it in terms of POPI;
- 1.17. **"Personal Information Impact Assessment"** means the forms adopted by the Company from time to time for performing assessments to determine the impact of processing operations on the Company and to identify risks;
- 1.18. **"Policy"** means this Protection of Personal Information ("POPI") Policy and any addendum thereto as may be amended by the Company;
- 1.19. **"POPI"** means the Protection of Personal Information Act, 3 of 2014;
- 1.20. **"Processing"** means the act of processing information includes any activity or any set of operations, whether or not by automatic means, concerning personal information and includes:
- 1.20.1. the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
- 1.20.2. dissemination by means of transmission, distribution or making available in any other form; or

- 1.20.3. merging, linking, as well as any restriction, degradation, erasure or destruction of information.
- 1.21. **“Re-Identify”** means 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;
- 1.22. **“Record”** Means any recorded information, regardless of form or medium, including:
- 1.22.1 Writing on any material;
  - 1.22.2 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;
  - 1.22.3 Label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;
  - 1.22.4 Book, map, plan, graph or drawing;
  - 1.22.5 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.
- 1.23. **“Regulations”** means the Regulations relating to POPI;
- 1.24. **“Responsible Party”** means the entity that determines the purpose of and means for processing the Personal Information;
- 1.25. **“Special Personal Information”** shall have the meaning assigned to it in terms of POPI;
- 1.26. **“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. INTRODUCTION**

- 2.1. 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 ("POPI").
- 2.2. POPI 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.
- 2.3. Through the provision of quality goods and services, the Company is necessarily involved in the collection, use and disclosure of certain aspects of the Personal Information of Clients, Customers, Employees and other stakeholders.
- 2.4. A person's right to privacy entails having control over his, her or its Personal Information and being able to conduct his or her affairs relatively free from unwanted intrusions.
- 2.5. Given the importance of privacy, the Company is committed to effectively managing Personal Information in accordance with POPI's provisions.
- 2.6. This policy describes the Company's guidelines with regard to:-
  - 2.6.1. Use Personal Information in the office;
  - 2.6.2. Access to and disclosure of Personal Information sent or received by employees or contractors of the Company with use of the Company email system;
  - 2.6.3. The Processing of Personal Information; and
  - 2.6.4. How to protect the Company from the risks of breach of security and/or unauthorized access to Personal Information.

## **3. PURPOSE**

- 3.1. This purpose of this policy is to protect the Company from the compliance risks associated with the Processing of Personal Information which includes:
  - 3.1.1 Breaches of confidentiality. For instance, the Company could suffer loss in revenue where it is found that the Personal Information of Data Subjects has been shared or disclosed inappropriately.

- 3.1.2. Failing to offer choice. For instance, all Data Subjects should be free to choose how and for what purpose the company uses information relating to them.
  - 3.1.3. Reputational damage. For instance, the Company could suffer a decline in shareholder value following an adverse event such as a computer hacker deleting the Personal Information held by the Company.
- 3.2. This policy demonstrates the Company's commitment to protecting the privacy rights of Data Subjects in the following manner:
  - 3.2.2. Through stating desired behaviour and directing compliance with the provisions of POPIA and best practices;
  - 3.2.3. By cultivating a company culture that recognises privacy as a valuable human right;
  - 3.2.4. By developing and implementing internal controls for the purpose of managing the compliance risks associated with the Processing of Personal Information;
  - 3.2.5. 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 the Company;
  - 3.2.6. By assigning specific duties and responsibilities to persons within the organisation, including the appointment of an Information Officer and Deputy Information Officers in order to protect the interests of the organisation and Data Subjects; and
  - 3.2.7. By raising awareness through training and providing guidance to individuals who process Personal Information so that they can act confidently and consistently.

#### **4. APPLICABILITY**

- 4.1. This policy applies to:
  - 4.1.1. The Directors;
  - 4.1.2. All branches, business units and divisions of the Company;



- 4.1.3. All Employees and volunteers;
- 4.1.4. All contractors, suppliers and other persons acting on behalf of the Company;
- 4.1.5. Operators who process Personal Information on the Company's instructions.
- 4.2. The policy must be read in conjunction with POPIA as well as the company's PAIA Manual 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:
  - 4.3.1. A Processing of:
    - 4.3.1.1. Personal Information;
    - 4.3.1.2. entered into a Record;
    - 4.3.1.3. by or for a Responsible Person;
    - 4.3.1.4. who is domiciled in South Africa.
- 4.4. POPIA does not apply in situations where the processing of Personal Information is concluded in the course of purely personal or household activities, or where the Personal Information has been de-identified.

## **5. INFORMATION OFFICER AND DEPUTY INFORMATION OFFICER**

- 5.1. The Company appoints Michiel Christiaan Erasmus as its Information Officer.
- 5.2. The Company duly appoints Christiaan Anton Frederik Morkel and Daniël Johannes de Waal as its Deputy Information Officers.
- 5.3. All Employees and/or Contractors may refer any queries, concerns or information of potential or actual breaches of Personal Information to the Deputy Information Officers.

## **6. DE-IDENTIFYING PERSONAL INFORMATION**

- 6.1. The Company has a responsibility to ensure that information that is outdated or no longer needed, is discarded in manner that will no longer identify the Data Subject.

- 6.2. Archived information records will be stored securely and a certificate of destruction will be obtained for each archived file/batch of Personal Information destroyed.
- 6.3. Each Employee and/or Contractor is required to take all the necessary precautions to ensure the abovementioned protocols are adhered to. Should the Company receive any complaints of failure to protect the Data Subject's information or properly respond to Data Subject requests, the claim must be disproved before the Information Officer. The result thereof is that the Employees and/or Contractors tasked with handling the information in question will be found guilty of contravening this Policy, the penalty thereof could lead to disciplinary action.
- 6.4. The Company's complaints procedure that should be followed in the event of a complaint is as follows:
  - 6.4.1. The complaint must be reported to one of the Deputy Information Officers immediately;
  - 6.4.2. The Deputy Information Officer must report the complaint to the other Deputy Information Officers and the Information Officer;
  - 6.4.3. The Employees and/or Contractors implicated must furnish the Information Officer with written representations of the Employees and/or Contractors) statement under oath;
  - 6.4.4. The Information Officer will liaise with the Regulator if necessary.

## **7. RIGHTS OF DATA SUBJECTS**

- 7.1. Where appropriate, the Company will ensure that its Clients and customers are made aware of the rights conferred upon them as Data Subjects in terms of POPI.

The Company will ensure that it gives effect to the following seven rights:

### **7.2. The Right to Access Personal Information**

- 7.2.1. The Company recognises that a Data Subject has the right to establish whether the Company holds Personal Information related to him, her or it including the right to request access to that Personal Information.

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

**7.3. The Right to have Personal Information Corrected or Deleted**

7.3.1. The Data Subject has the right to request, where necessary, that his, her or its Personal Information must be corrected or deleted where the Company is no longer authorised to retain the Personal Information.

**7.4. The Right to Object to the Processing of Personal Information**

7.4.1. The Data Subject has the right, on reasonable grounds, to object to the processing of his, her or its Personal Information.

7.4.2. In such circumstances, the Company will give due consideration to the request and the requirements of POPI. The Company 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.

**7.5. The Right to Object to Direct Marketing**

7.5.1. 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.

**7.6. The Right to Complain to the Information Regulator**

7.6.1. 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 POPI and to institute civil proceedings regarding the alleged noncompliance with the protection of his, her or its Personal Information.

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

**7.7. The Right to be Informed**

7.7.1. The Data Subject has the right to be notified that his, her or its Personal Information is being collected by the Company.

7.7.2. The Data Subject also has the right to be notified in any situation where the company has reasonable grounds to believe that the personal information

of the data subject has been accessed or acquired by an unauthorised person.

- 7.8. Employees will be required to assist the Information Officer and/or Deputy Information Officers in processing Data Subject requests made under the provisions of POPI or PAIA, if instructed from time to time.

## **8. REQUIREMENTS FOR LAWFUL PROCESSING**

All Employees and persons acting on behalf of the Company will at all times be subject to, and act in accordance with, the following guiding principles:

### **8.1. Accountability**

- 8.1.1. The Company is legally responsible for any Personal Information in its possession or under its control.
- 8.1.2. Failing to comply with POPIA could potentially damage the Company's reputation or expose the Company to a civil claim for damages. The protection of Personal Information is therefore everybody's responsibility.
- 8.1.3. Every person who is subject to this policy are required to take responsibility for the Personal Information Processed by him/her/it and to ensure that it is handled in a lawful and secure manner.
- 8.1.4. The Company 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.

### **8.2. Processing Limitation**

- 8.2.1. The Company will ensure that Personal Information under its control is processed:
- 8.2.1.1. in a fair, lawful and non-excessive manner, and
- 8.2.1.2. only with the informed consent of the Data Subject unless otherwise justified in terms of POPI, and
- 8.2.1.3. only for a specifically defined purpose.

8.2.2. The Company will inform the Data Subject of the reasons for collecting his, her or its Personal Information and take steps to obtain written consent prior to processing Personal Information, unless processing is based on an alternative lawful ground provided in POPI.

8.2.3. The Company will under no circumstances distribute or share Personal Information between separate legal entities, associated Company's (such as subsidiary companies) or with any individuals that are not directly involved with facilitating the purpose for which the information was originally collected.

8.2.4. Where applicable, the Data Subject must be informed of the possibility that their Personal Information will be shared with other aspects of the Company's business and be provided with the reasons therefor.

### 8.3. **Purpose Specification**

8.3.1. The Company will process Personal Information only for specific, explicitly defined and legitimate reasons which are related to its normal business functions.

8.3.2. The Company will inform Data Subjects of these reasons prior to collecting or recording the data subject's personal information.

### 8.4. **Further Processing Limitation**

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

8.4.2. Therefore, where the company 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 Company will first obtain additional consent from the Data Subject.

### 8.5. **Information Quality**

8.5.1. The Company will take reasonable steps to ensure that all Personal Information collected is complete, accurate and not misleading.

- 8.5.2. Where appropriate, Personal Information must be verified with reference to acceptable supporting documentation (i.e. ID copies or proof of residence).
- 8.5.3. Where Personal Information is collected or received from third parties, the company 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.

## 8.6. **Openness**

- 8.6.1. The Company will take reasonable steps to ensure that Data Subjects are notified (are at all times aware) that their Personal Information is being collected including the purpose for which it is being collected and Processed.
- 8.6.2. The Company can be contacted on the following email addresses: [hdw@esattorneys.co.za](mailto:hdw@esattorneys.co.za); [caf@esattorneys.co.za](mailto:caf@esattorneys.co.za) to:
  - 8.6.2.1. Enquire whether the Company holds related Personal Information, or
  - 8.6.2.2. Request access to related Personal Information, or
  - 8.6.2.3. Request the Company to update or correct related Personal Information, or
  - 8.6.2.4. Make a complaint concerning the Processing of Personal Information.

## 8.7. **Security Safeguards**

- 8.7.1. The Company will manage the security of its Records and Filing Systems 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.
- 8.7.2. The Company will continuously review its security controls which will include regular testing of protocols and measures put in place to combat cyber-attacks on the Company's IT network.

- 8.7.3. The Company will ensure that all paper and electronic records comprising Personal Information are securely stored and made accessible only to authorised individuals.
- 8.7.4. All new Employees will be required to sign employment contracts incorporating 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 Company is responsible.
- 8.7.5. All existing Employees will, after the required consultation process has been followed, be required to sign an addendum to their employment containing the relevant notice, consent and confidentiality clauses.
- 8.7.6. The Company's operators and third-party service providers will be required to enter into Operator Agreements with the Company where both parties pledge their mutual commitment to POPIA and the lawful processing of any Personal Information pursuant to the main agreement between the Parties.
- 8.7.7. Written Records will be kept secure:**
- 8.7.7.1. Personal Information records should be kept in locked filing rooms, locked cabinets, or safes;
- 8.7.7.2. When in use Personal Information Records should not be left unattended in areas where non-staff members may access them;
- 8.7.7.3. The Company shall implement and maintain a "Clean Desk Policy" where all staff shall be required to clear their desks of all Personal Information any kind when leaving their desks for any length of time and at the end of the day;
- 8.7.7.4. Personal Information which is no longer required should be disposed of by shredding in accordance with the Company's Records Retention and Destruction Policy;
- 8.7.7.5. No Records shall be removed from paper-based files without the explicit permission of the Information Officer;

8.7.7.6. Records that were placed on files shall not be altered without consent. Should evidence be obtained of tampering with records, the staff member involved shall be subject to disciplinary action.

8.7.7.7. To give effect to the above, Employees shall:

8.7.7.7.1. Close and lock doors when leaving their offices unattended;

8.7.7.7.2. Lock file cabinets that store Personal Information;

8.7.7.7.3. Don't leave Personal Information in plain view at desks or on a whiteboard;

8.7.7.7.4. Don't leave Personal Information sitting on a printer, copier, fax machine or other peripheral device;

8.7.7.7.5. Do not take records home without prior consent from management;

8.7.7.7.6. Any loss or theft of, or unauthorised access to, Personal Information must be immediately reported to the Deputy Information Officers.

**8.7.8. Electronic records of any kind will be kept secure:**

The Company shall use systems which ensure that its electronic records are authentic; not altered or tampered with; legible; auditable; and produced/processed in systems which utilise security measures to ensure their integrity, including:

8.7.8.1. All electronically held Personal Information must be saved in a secure database;

8.7.8.2. As far as reasonably practicable, no Personal Information of Data Subjects of the Company should be saved on personally owned computers, laptops or hand-held devices, unless prior consent is obtained from management;

8.7.8.3. All computers, laptops and hand-held devices should be access protected with a password of at least 16 characters, fingerprint



or with the password or screen finger scan being of reasonable complexity and changed frequently;

- 8.7.8.4. Company Personal Information may not be stored on personally
- 8.7.8.5. owned devices, except with the prior written consent of the Deputy Information Officers;
- 8.7.8.6. Company Personal Information may not be stored on CDs, DVDs, USBs, etc. Where possible the functionality to insert removable storage in a computer or similar device should be disabled;
- 8.7.8.7. Personal Information may not be transmitted via email or other insecure messaging solutions without the consent of the Data Subject or other lawful ground for processing;
- 8.7.8.8. Employees may not use their personal email for business communications;
- 8.7.8.9. Strong passwords or passphrases must be used by all Employees. Requirements for strong passwords:
  - 8.7.8.9.1. 16 characters minimum;
  - 8.7.8.9.2. Avoid using the same password for multiple accounts;
  - 8.7.8.9.3. Don't write your password down or store it in an insecure manner;
  - 8.7.8.9.4. Don't share your password with anyone for any reason;
  - 8.7.8.9.5. Never let anyone use your password to log into a system;
  - 8.7.8.9.6. Never share your passwords with co-workers while on vacation; and
  - 8.7.8.9.7. Don't use automatic login functionality.

- 8.7.8.10. Employees must ensure that their work computer or laptop has approved virus protection installed and regularly update same;
- 8.7.8.11. Employees must avoid opening attachments from an untrusted sources; clicking on links in electronic communications from an untrusted source;
- 8.7.8.12. Employees have to ensure that they know the common ways to spot phishing scams;
- 8.7.8.13. All staff of the Company shall implement and maintain a "Clean Screen Policy" where all employees shall be required to lock their computers or laptops when leaving their desks for any length of time and to log off at the end of the day. Automatic locking must be enabled on computers after 15 minutes of no activity.
- 8.7.8.14. Electronic Personal Information which is no longer required must be deleted from the individual laptop, handheld device and/or computer and the relevant database. The Employee must ensure that the information has been completely deleted and is not recoverable. Any loss or theft of computers, laptops or other devices which may contain Personal Information must be immediately reported to the Information Officer, who shall notify the IT department, who shall take all necessary steps to remotely delete the information, if possible.

**8.7.9. Passwords and Access:**

- 8.7.9.1. Users have a responsibility to safeguard any credentials granted to them by the Company. In order to limit security risks, all Employees and Directors must abide by the following:
  - 8.7.9.1.1. Attempts should not be made to by-pass or render ineffective security measures provided by the Company.
- 8.7.9.2. Users may not:
  - 8.7.9.2.1. Share user IDs or usernames.

- 8.7.9.2.2. Divulge passwords to other users.
- 8.7.9.2.3. Attempt to impersonate other users.
- 8.7.9.2.4. Leave their computer unattended without logging out or locking
- 8.7.9.2.5. Share passwords between users, except where they are released as part of the approved procedure. An approved procedure exists for releasing passwords where accounts are required, and staff are unavailable.

**8.7.10. Online Activities:**

- 8.7.10.1. All Employees have a responsibility to avoid risky behaviour online by, *inter alia*:
  - 8.7.10.1.1. Being cautious when using file sharing applications;
  - 8.7.10.1.2. Applications;
  - 8.7.10.1.3. Not downloading software or applications from the internet without authorization from management;
  - 8.7.10.1.4. Being cautious when browsing the web;
  - 8.7.10.1.5. Being cautious when clicking on shortened URL's;
  - 8.7.10.1.6. Not using Torrent sites; and
  - 8.7.10.1.7. Avoiding responding to questions or clicking on links in pop-up windows.

**8.7.11. Protecting Verbal Communication:**

- 8.7.11.1. Employees must not divulge Confidential or Personal Information to any third party unless he/she is permitted to do so in terms of this Policy. If permitted, he/she must be mindful

of their surroundings and ensure that unauthorised persons don't gain access to same.

**8.8. Data Subject Participation:**

- 8.8.1. A Data Subject may request the correction or deletion of his, her or its Personal Information held by the Company.
- 8.8.2. The Company will ensure that it provides a facility for Data Subjects who want to request the correction or deletion of their Personal Information.
- 8.8.3. Where applicable, the Company will include a link to unsubscribe from any of its electronic newsletters or related marketing activities.

**9. ACCESS AND SECURITY TO INFORMATION/RECORDS**

- 9.1. Records in all formats, shall at all times be protected against unauthorised access and tampering to protect their authenticity and reliability as evidence of the business of the Company.
- 9.2. Records shall be managed only by authorised persons.
- 9.3. No staff member shall remove records in any format that are not available in the public domain from the premises of the Company without the explicit permission of the Information Officer.
- 9.4. No staff member shall provide information and records that are not in the public domain to the public without consulting the Information Officer. Specific guidelines regarding requests for information are contained in the POPI/PAIA Manual which is maintained by the Information Officer.
- 9.5. Personal Information shall be managed in terms of the policy and POPI.
- 9.6. No staff member shall disclose Personal Information of any member of staff or any other Data Subject to any member of the public without the express prior consent of the Information Officer.

**10. TECHNICAL AND ORGANISATIONAL MEASURES**

- 10.1. The Company has developed a Compliance Management Framework to:

- 10.1.1. Help the Company secure Personal Information against data breaches, leaks, or other incidents where an unauthorized party could gain access to it;
  - 10.1.2. Identify risks to the security of the Company's equipment, premises, systems, networks, and other means of processing personal information; and
  - 10.1.3. Minimize security risks, including through Personal Information Impact Assessments and monitoring.
- 10.2. The Company will assign duties to Employees within the Company, and where appropriate, to external persons to ensure the proper implementation of the framework.
- 10.3. The following technical and organizational measures will be implemented by the Company:

**10.3.1. Physical Controls**

- 10.3.1.1. **Physical access measures:** locking filing cabinets or office doors and physical access controls (such as key cards, biometrics, or other identification methods to ensure that only authorized persons have access);
- 10.3.1.2. **Physical monitoring:** video surveillance (CCTV systems) and security personnel;
- 10.3.1.3. **Hard copy records management:** shredding paper records which are no longer needed in a safe manner and enforcing clean desk policies;
- 10.3.1.4. **Physical privacy measures:** having private consulting and storage areas; and
- 10.3.1.5. **Ancillary physical measures** that physically limit or prevent access to data, be it on IT equipment, systems, or infrastructure, or in hard copy records.

**10.3.2. Technical Controls**

- 10.3.2.1. **Data security:** file encryption and password protection, export control and data classification;

- 10.3.2.2. **Equipment and systems security:** device and removable storage media encryption, user access management, mobile device management and secure disposal or re-use of equipment;
- 10.3.2.3. **Network and communications security:** firewalls, end-to-end encryption, digital access control, penetration testing and endpoint protection;
- 10.3.2.4. **Software security:** antivirus software and keeping software up to date; and
- 10.3.2.5. **Other measures** related to hardware or software that protects systems and resources.

### **10.3.3. Operational controls**

- 10.3.3.1. **Operational awareness:** fostering a culture of data protection through an Employee awareness campaign;
- 10.3.3.2. **Training:** in-house and external (where appropriate) training to operationalize policies;
- 10.3.3.3. **Operational monitoring:** monitoring workstations and providing a way of reporting data breaches;
- 10.3.3.4. **Procedures:** employee on-boarding and exit and security procedures;
- 10.3.3.5. **Other measures** that involve members of the Company.

### **10.3.4. Administrative controls**

- 10.3.4.1. **Administrative awareness:** director awareness and impressing management responsibility;
- 10.3.4.2. **Security planning:** planning around data protection, business continuity arrangements and considering acceptable standards;
- 10.3.4.3. **Security documentation:** drafting the necessary data protection policies and updating them regularly;

10.3.4.4. **Security assurances:** cyber insurance (if appropriate), implementing due diligence (risk assessment) procedures and implementing audit controls; and

10.3.4.5. **Other measures** that involve senior management.

**10.3.5. Continued review**

10.3.5.1. The Information Officer and relevant Employees will continually review:

10.3.5.1.1. The security of equipment, premises, systems, networks;

10.3.5.1.2. The adequacy of the information security framework;

10.3.5.1.3. Against industry security standards.

**11. PERFORMING A POPI GAP ANALYSIS AND RISK ASSESSMENTS**

11.1. The Company already takes care when processing data. However, the Company has to identify what areas of POPI compliance the Company already meets and where the Company is deficient.

11.2. POPIA's security requirements require the Information Officer of the Company to take necessary measures for protecting the Company's information.

11.3. Risk Assessment/Gap Analysis is an opportunity to identify the Company's security strengths and weaknesses, and to ensure that management can cope with the information security threats the Company faces.

11.4. The risk assessment, is also an analysis of how Personal Information is collected, used, shared, stored, filed and maintained by the Company.

11.5. The Gap Analysis can reveal where the Company has weaknesses when it comes to protecting the Personal Information it collects, stores and uses.

11.6. Processes have to be put in place to collect data only for a specific purpose: to inform the Data Subjects of the reason for collection, and to have a process for safely deleting/destroying the data when it has served its purpose.

- 11.7. The gap analysis and risk assessments should normally be started early in project development or design, or before a new data processing activity, and must be considered throughout the information lifecycle from collection to destruction.
- 11.8. To sum it up, here are some questions to answer when the Company is undertaking assessments:
- 11.8.1. Does the Company have the appropriate legal authority to collect personal data?
  - 11.8.2. Have the Company received consent from the data subjects to use their data?
  - 11.8.3. Is the Company using out-of-date or irrelevant personal data to make decisions?
  - 11.8.4. Is the Company disclosing data to third parties that it is not authorised or who do not keep personal data appropriately secure?
  - 11.8.5. Do the Company have processes in place to dispose of private data after use?
- 11.9. The Deputy Information Officers have adopted a prescribed form for conducting impact and risk assessments which will be used when deemed appropriate to maintain the Company's compliance with POPI.

## **12. POPI AND E-MAIL USAGE**

- 12.1. If it is needed, each Employee within the Company is provided with a Company email account to assist with their work for the Company. This account is the primary way that Employees will communicate with Clients and other Data Subjects.
- 12.2. The email account of an Employee, and any information contained in it, including content, headers, directories and email system logs, remains the property of the Company.
- 12.3. Usage of the Company email system is exclusively for Company and professional purposes.
- 12.4. Incidental use of an e-mail account for personal purposes is allowed and is subject to the same policies and regulations as official use. However, systematic use on behalf of



individuals or organisations that are not associated with the Company or its business is not allowed.

- 12.5. Employees are responsible for the integrity of their mailbox. IT Services cannot restore any emails deleted accidentally or otherwise. All email messages may be
- 12.6. subject POPI and other legislation and laws of South Africa and any employment prescripts as amended, updated or replaced from time to time.
- 12.7. Although the Company has systems in place to protect the integrity and safety of the Company's electronic network, it must be noted that the Company cannot guarantee the confidentiality of the information stored on any network device belonging to the Company.
- 12.8. Great care should be taken when attaching documents to ensure the correct information is being released.
- 12.9. Any email should be regarded as a written formal letter and information.
- 12.10. Employees should take care when carbon copying (CC) persons in email correspondence which is not directly addressed to them. Further care should be taken to avoid disclosure of client contact information to third parties when copying them in emails. If email correspondence directly concerns a Client, the blind copying (BCC) function should be used.
- 12.11. Any defamatory or careless remarks can have very serious consequences. The use of indecent, obscene, sexist, racist or other inappropriate remarks whether in written form, in cartoon form or otherwise, is strictly prohibited.
- 12.12. To prevent computer viruses being transmitted through the network, care must be taken when dealing with suspect e-mails and attachments of unknown origin are received. Suspect e-mails should be deleted immediately and never forwarded to other Users.
- 12.13. E-mail users must be aware of the use of dangerous code by hackers and other outside parties which refers to any computer program that causes destruction or harm and has been programmed in such a way with the malicious intent of the content of a computer or other electronic communication device. Dangerous Code is classified as file infector viruses, system or boot record viruses and macro viruses. It must be noted that viruses can either be decimated or "contracted" by the exchange of various media or by the receipt in an e-mail from a source that is unknown or spam. Effective anti-virus software will normally indicate such e-mails.

- 12.14. Staff are not authorised to retrieve or read any e-mail messages that are not sent to them or not for their attention, except when authorised under the approved procedure.
- 12.15. Email messages must not be forwarded to external non-Company accounts such as a staff member's own personal e-mail account. Should a staff member or learner receive any offensive, unpleasant, harassing or intimidating messages via e-mail, he/she are requested to inform the Information Officer immediately.

### **13. COMPLIANCE MANAGEMENT FRAMEWORK**

- 13.1. Compliance is not a "one-and-done event". It is an ongoing and active process that requires consistent management. The Company should have an active compliance plan in place that provides for a systematic way to review and update the Company's processing standards on a regular basis.

### **14. PROCESSING OF INFORMATION BY USING AUTOMATED AND NON-AUTOMATED MEANS**

- 14.1. POPIA applies to the processing of any Personal Information by the Company that has been entered into a record by or for the Company as the responsible party by using automated and non-automated means.
- 14.2. This is subject to the proviso that when the recorded Personal Information is processed by any non-automated means, the record must form part of a filing system or is intended to form part of a filing system. Due to the wide definition of a "filing system" contained in POPI, all Personal Information should be handled according to this Policy unless it is expressly excluded by management.

### **15. SPECIFIC DUTIES AND RESPONSIBILITIES**

#### **15.1. Board of Directors/Senior Management**

- 15.1.1. The Company's Directors cannot delegate their accountability and are ultimately answerable for ensuring that the Company meets its legal obligations in terms of POPI.
- 15.1.2. The Directors may however delegate some of their responsibilities in terms of POPI to management or other capable individuals.
- 15.1.3. The Directors are responsible for ensuring that:

- 15.1.3.1. The Company appoints an Information Officer, and where necessary, a Deputy Information Officer.
- 15.1.3.2. All persons responsible for the Processing of Personal Information on behalf of the company:
  - 15.1.3.2.1. are appropriately trained and supervised to do so,
  - 15.1.3.2.2. 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.
  - 15.1.3.2.3. 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.
  - 15.1.3.2.4. The scheduling of a periodic POPI Audit in order to accurately assess and review the ways in which the company collects, holds, uses, shares, discloses, destroys and processes personal information.

## 15.2. **Information Officer**

- 15.2.1. The Company's Information Officer is responsible for:
  - 15.2.1.1. Taking steps to ensure the company's reasonable compliance with the provision of POPIA.
  - 15.2.1.2. Keeping the governing body updated about the company's 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.
  - 15.2.1.3. Continually analysing privacy regulations and aligning them with the company's personal information processing

procedures. This will include reviewing the company's information protection procedures and related policies.

- 15.2.1.4. Ensuring that POPI Audits are scheduled and conducted on a regular basis.
- 15.2.1.5. Ensuring that the company makes it convenient for data subjects who want to update their personal information or submit POPI related complaints to the company. For instance, maintaining a "contact us" facility on the company's website.
- 15.2.1.6. Approving any contracts entered into with operators, employees and other third parties which may have an impact on the personal information held by the company. This will include overseeing the amendment of the company's employment contracts and other service level agreements.
- 15.2.1.7. Encouraging compliance with the conditions required for the lawful processing of personal information.
- 15.2.1.8. Ensuring that employees and other persons acting on behalf of the company are fully aware of the risks associated with the processing of personal information and that they remain informed about the company's security controls. Organising and overseeing the awareness training of employees and other individuals involved in the processing of personal information on behalf of the company.
- 15.2.1.9. Addressing employees' POPIA related questions.
- 15.2.1.10. Addressing all POPIA related requests and complaints made by the company's data subjects.
- 15.2.1.11. 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.
- 15.2.1.12. To ensure that:-

- 15.2.1.12.1. A Compliance Framework is developed, implemented, monitored and maintained;
  - 15.2.1.12.2. A Personal Information Impact Assessment is done to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of Personal Information;
  - 15.2.1.12.3. A manual is developed, monitored, maintained and made available as prescribed in terms of sections 14 and 51 of PAIA, as amended;
  - 15.2.1.12.4. Internal measures are developed together with adequate systems to process requests for information and access thereto;
  - 15.2.1.12.5. Internal awareness sessions are conducted regarding the provisions of POPI, Regulations, codes of conduct (if applicable) or information obtained from the Information Regulator; and
  - 15.2.1.12.6. Upon request by any person, copies of the manual are provided to that person upon payment of a fee to be determined by the Regulator from time to time;
  - 15.2.1.12.7. A report is submitted to the Information Regulator annually regarding the aspects set out in Regulation 6.3;
  - 15.2.1.12.8. If requested by the Information Regulator, to furnish it with information about requests for access to the records of the company.
- 15.2.2. To monitor the execution of delegated duties by the Deputy Information Officer.
- 15.2.3. The Deputy Information Officer will assist the Information Officer in performing his or her duties.

### 15.3. IT Manager

15.3.1. The company's IT Manager is responsible for:

- 15.3.1.1. Ensuring that the company's IT infrastructure, filing systems and any other devices used for Processing Personal Information meet acceptable security standards.
- 15.3.1.2. Ensuring that all electronically held Personal Information is kept only on designated drives and servers and uploaded only to approved cloud computing services.
- 15.3.1.3. Ensuring that servers containing Personal Information are sited in a secure location, away from the general office space.
- 15.3.1.4. Ensuring that all electronically stored Personal Information is backed-up and tested on a regular basis.
- 15.3.1.5. Ensuring that all back-ups containing Personal Information are protected from unauthorised access, accidental deletion and malicious hacking attempts.
- 15.3.1.6. Ensuring that Personal Information being transferred electronically is encrypted.
- 15.3.1.7. Ensuring that all servers and computers containing Personal Information are protected by a firewall and the latest security software.
- 15.3.1.8. Performing regular IT audits to ensure that the security of the company's hardware and software systems are functioning properly.
- 15.3.1.9. Performing regular IT audits to verify whether electronically stored Personal Information has been accessed or acquired by any unauthorised persons.
- 15.3.1.10. Performing a proper due diligence review prior to contracting with operators or any other third-party service providers to process personal information on the company's behalf. For instance, cloud computing services.

#### **15.4. Marketing and Communication Manager**

15.4.1. The company's Marketing & Communication Manager is responsible for:

15.4.1.1. Approving and maintaining the protection of Personal Information statements and disclaimers that are displayed on the Company's website, including those attached to communications such as emails and electronic newsletters.

15.4.1.2. Addressing any Personal Information protection queries from journalists or media outlets such as newspapers.

15.4.1.3. Where necessary, working with persons acting on behalf of the Company to ensure that any outsourced marketing initiatives comply with POPI.

#### **15.5. Employees and other Persons acting on behalf of the Company**

15.5.1. Employees and other persons acting on behalf of the Company 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.

15.5.2. Employees and other persons acting on behalf of the Company are required to treat Personal Information as a confidential business asset and to respect the privacy of Data Subjects.

15.5.3. Employees and other persons acting on behalf of the Company may not directly or indirectly, utilise, disclose or make public in any manner to any person or third party, either within the Company 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.

15.5.4. Employees and other persons acting on behalf of the Company 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.

15.5.5. Employees and other persons acting on behalf of the Company will only process personal information where:

- 15.5.5.1. The Data Subject, or a competent person where the data subject is a child, consents to the processing; or
  - 15.5.5.2. 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
  - 15.5.5.3. The processing complies with an obligation imposed by law on the responsible party; or
  - 15.5.5.4. The processing protects a legitimate interest of the Data Subject; or
  - 15.5.5.5. The Processing is necessary for pursuing the legitimate interests of the company or of a third party to whom the information is supplied.
- 15.5.6. Furthermore, Personal Information will only be processed where the Data Subject:
- 15.5.6.1. Clearly understands why and for what purpose his, her or its Personal Information is being collected; and
  - 15.5.6.2. Has granted the Company with explicit written or verbally recorded consent to process his, her or its Personal Information.
- 15.5.7. Employees and other persons acting on behalf of the company 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.
- 15.5.8. 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.
- 15.5.9. Consent can be obtained in written form which includes any appropriate electronic medium that is accurately and readily reducible to printed form. Alternatively, the Company will keep a voice recording of the Data Subject's consent in instances where transactions are concluded telephonically or via electronic video feed.



- 15.5.10. Consent to process a Data Subject's Personal Information will be obtained directly from the Data Subject, except where:
  - 15.5.10.1. the Personal Information has been made public, or
  - 15.5.10.2. where valid consent has been given to a third party, or
  - 15.5.10.3. the information is necessary for effective law enforcement.
- 15.5.11. Employees and other persons acting on behalf of the Company will under no circumstances:
  - 15.5.11.1. 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.
  - 15.5.11.2. 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 the company's central database or a dedicated server.
  - 15.5.11.3. Share Personal Information informally. In particular, 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.
  - 15.5.11.4. Transfer Personal Information outside of South Africa without the express permission from the Information Officer.
- 15.5.12. Employees and other persons acting on behalf of the company are responsible for:
  - 15.5.12.1. Keeping All Personal Information that they come into contact with secure, by taking sensible precautions and following the guidelines outlined within this policy;
  - 15.5.12.2. 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;

- 15.5.12.3. 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 the company, with the sending or sharing of Personal Information to or with authorised external persons;
- 15.5.12.4. 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;
- 15.5.12.5. Ensuring that their computer screens and other devices are switched off or locked when not in use or when away from their desks;
- 15.5.12.6. 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;
- 15.5.12.7. 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;
- 15.5.12.8. 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.
- 15.5.12.9. 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;
- 15.5.12.10. 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;

15.5.12.11. 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;

15.5.12.12. Undergoing POPI Awareness training from time to time;

15.5.12.13. Where an Employee, or a person acting on behalf of the company, 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.

## **16. REQUEST TO ACCESS PERSONAL INFORMATION PROCEDURE**

16.1. Data subjects have the right to:

16.1.1. Request what personal information the Company holds about them and why;

16.1.2. Request access to their Personal Information;

16.1.3. Be informed how to keep their personal information up to date;

16.1.4. 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";

16.1.5. 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 company's PAIA Policy;

16.1.6. The Information Officer will process all requests within a reasonable time.

## **17. FORBIDDEN USES OF DATA SUBJECT'S PERSONAL INFORMATION**

17.1. The Employee or Contractor may not use the Company's access to any Data Subject's Personal Information for personal gain on any such purposes as soliciting or proselytizing for commercial ventures, religious or personal causes or outside organizations or other similar, non-job-related solicitations. If the Company discovers that any Employee or Contractor misusing the information available in the Company's systems, that particular Employee and/or Contractor will be subject to disciplinary action, which may include dismissal.

17.2. Should an Employee or Contractor be suspected of contravening this policy, the Company may at its sole discretion access any device which the Employee or Contractor uses to conduct business to investigate the matter further.

### **17.3. Common Acts of POPI Non-Compliance:**

17.3.1. Loss or theft of paperwork/data/misfiling/not saving data;

17.3.2. Data posted or e-mailed or sent to the incorrect recipient including on any groups on any social media application or platform;

17.3.3. Insecure webpage (including hacking);

17.3.4. Loss or theft of an unencrypted device;

17.3.5. No or inadequate firewalls and/or anti-virus software.;

17.3.6. Insecure disposal of paperwork;

17.3.7. Failure to redact data;

17.3.8. Sensitive or confidential information uploaded to the webpage;

17.3.9. Verbal disclosure without permission or carelessly done;

17.3.10. Insecure disposal of hardware;

17.3.11. Sending confidential data by e-mail/Apps that are not supposed to be circulated;

- 17.3.12. Sticky notes with Personal Information such as passwords or reminders left in unsecure areas;
- 17.3.13. Smartphone unsecured data breach;
- 17.3.14. Lost keys data breach/not keeping keys safe;
- 17.3.15. Lost digital/electronic items data breach (laptops, USBs, external hard drives etc.);
- 17.3.16. Easy access to computer room/offices;
- 17.3.17. Leaving file cabinets, desk drawers and cupboards open or documents on desks unattended;
- 17.3.18. Unsecured access card;
- 17.3.19. Forgotten documents in the printer/copy machine;
- 17.3.20. Responding to phishing e-mails/clicking on unsecured links.

## **18. COMPANY'S RIGHT TO ACCESS INFORMATION**

- 18.1. The Company respects the individual privacy of its Employees and/or Contractors. However, Employee and/or Contractor privacy does not extend to the Employee's and/or Contractor's work-related conduct or to the use of Company provided equipment or supplies.
- 18.2. The electronic mail system has been installed by the Company to facilitate business communications. Although each Employee and/or Contractor has an individual password to access this system, it belongs to the Company and the contents of email communications are accessible at all times by the Company management for any business purpose. These systems may be subject to periodic unannounced inspections and should be treated like other shared filing systems. All system passwords and encryption keys must be available to the Company management and the designated IT personnel, and the Employee and/or Contractor may not use passwords that are unknown to their supervisor or the designated IT personnel or install encryption programs without turning over encryption keys to their supervisor your designated IT personnel. All e-mail messages are Company records. The contents of email, properly obtained for legitimate business purposes, may be disclosed within the Company without the Employee's and/or Contractor's permission.

- 18.3. Therefore, the Employee and/or Contractor should not assume that messages or telephone calls are confidential. Back-up copies of e-mail may be maintained and referenced for business and legal reasons.

## **19. BREACH OF SECURITY/ UNAUTHORISED ACCESS TO INFORMATION**

- 19.1. Information Security Breaches will be handled strictly in accordance with the Company's Data Breach Management Policy.
- 19.2. Should the Company experience any security breach, it is required, by law, to notify the Regulator; and the Data Subject(s) whose information have been affected by the breach, unless the identity of such Data Subject(s) cannot be established.
- 19.3. Therefore, the Employee and/or Contractor should report any known or suspected breach of information to the appointed Information Officer.
- 19.4. Failure to report the aforementioned breach will subject the Employee and/or Contractor in transgression to disciplinary action, which may include dismissal.
- 19.5. The Company has established a complaints process to deal with allegations of leaked information. This will be addressed by the Deputy Information Officers.

## **20. CORPORATE POLICY GUIDELINE**

### **20.1. Acceptable Uses of Personal Information**

- 20.1.1. The Company provides access to its server and email access is intended to be for business reasons only. The Company encourages the use of the server and email because they make communication more efficient and effective. However, the server and e-mail are Company property, and their purpose is to facilitate Company business. Every Employee and/or Contractor has a responsibility to maintain and enhance the Company's public image and to use Company email and access to the server in a productive manner. To ensure that all Employees and/or Contractors are responsible, the following guidelines have been established for using email and the server. Any improper use of the server or e-mail is not acceptable and will not be permitted.

- 20.1.2. The Employee and/or Contractor acknowledges that:-

- 20.1.2.1. The Company may be held vicariously liable for the acts of its Employees and/or Contractors, even where the Company is not at fault, for any damages caused by the Employee's and/or Contractor's conduct;
- 20.1.2.2. Employees and/or Contractors may not make representations to third parties or the public beyond the scope of their normal responsibilities or actual authority;
- 20.1.2.3. Methods other than email must be used to communicate Special Personal Information.

## **20.2. Unacceptable Uses of Personal Information**

- 20.2.1. The Company acknowledges that Employees and/or Contractors need reasonable access to Data Subjects' Personal Information in order to fulfil their tasks.
- 20.2.2. The Employees and/or Contractors may not process the Employee's and/or Contractors' Personal Information without obtaining the requisite consent, following the protocols discussed in this policy and in the Act.

## **20.3. Queries and Clarification of Policy**

- 20.3.1. Where an Employee is uncertain as to the content of this policy or requests further clarification of issues which are addressed in this policy they are required to contact the Information Officer for clarification.

## **21. MONITORING AND IMPLEMENTATION OF THE POLICY**

- 21.1. The Information Officer, Deputy Information Officers, senior management and all operators, as defined by POPIA, are responsible for administering and overseeing the implementation of this policy and, as applicable, supporting guidelines, standard operating procedures, notices, consents and appropriate related documents and processes.
- 21.2. Periodic reviews and audits will be conducted by the Information Officer/Deputy Information Officer where appropriate, to demonstrate compliance with POPIA, any policies and guidelines.

## **22. POPI COMPLAINTS PROCEDURE**

Complaints may be filled via email to [hdw@esattorneys.co.za](mailto:hdw@esattorneys.co.za) /[caf@esattorneys.co.za](mailto:caf@esattorneys.co.za).

## **23. DISCIPLINARY ACTION**

- 23.1. Where a POPI complaint or a POPI infringement investigation has been finalised, the Company 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.
- 23.2. In the case of ignorance or minor negligence, the Company will undertake to provide further awareness training to the employee.
- 23.3. Any gross negligence or the wilful mismanagement of Personal Information, will be considered a serious form of misconduct for which the Company may summarily dismiss the employee. Disciplinary procedures will commence where there is sufficient evidence to support an Employee's gross negligence.
- 23.4. Examples of immediate actions that may be taken subsequent to an investigation include:
  - 23.4.1. A recommendation to commence with disciplinary action;
  - 23.4.2. A referral to appropriate law enforcement agencies for criminal investigation; and/or
  - 23.4.3. Recovery of funds and assets in order to limit any prejudice or damages caused.



## ANNEXURE A: PERSONAL INFORMATION REQUEST FORM

Please download, complete and email to DJ de Waal or CAF Morkel.

<b>Please submit the completed form to the deputy information officer:</b>	
Name	DJ de Waal / CAF Morkel
Contact Number	(012) 460 0396
Email address	<a href="mailto:hdw@esattorneys.co.za">hdw@esattorneys.co.za</a> / <a href="mailto:caf@esattorneys.co.za">caf@esattorneys.co.za</a>

Please be aware that we may require you to provide proof of identification prior to processing your request.

There may also be a reasonable charge for providing copies of the information requested.

<b>A. Particulars of Data Subject</b>	
Name & Surname	
Identity no	
Postal address	
Contact no	
Email address	
<b>B. Request</b>	
I request the Company to:	
(a) Inform me whether it holds any of my personal information	
(b) Provide me with a record or description of my personal information	
(c) Correct or update my personal information	
(d) Destroy or delete a record of my personal information	
<b>C. Instructions</b>	
<b>D. Signature</b>	
<b>Signature</b>	<b>Date:</b>

We need the Personal Information requested in this form to:

- Locate the requested information/documentation;
- Give effect to your request;
- Send you information/documentation;
- Contact you regarding your request;
- Record particulars of the Request in a register; and
- Other purposes directly related to the above.

**If the Personal Information described above is being processed by a third party on our behalf, you consent that we may disclose the information herein to such third party in order to comply with your request.**

## ANNEXURE B: POPI COMPLAINT FORM

Please download, complete and email to DJ de Waal or CAF Morkel.

We are committed to safeguarding your privacy and the confidentiality of your Personal Information and are bound by the Protection of Personal Information Act.

Please submit your complaint to the deputy information officer:	
Name	DJ de Waal / CAF Morkel
Contact Number	(012) 460 0396
Email address	<a href="mailto:hdw@esattorneys.co.za">hdw@esattorneys.co.za</a> / <a href="mailto:caf@esattorneys.co.za">caf@esattorneys.co.za</a>

Where we are unable to resolve your complaint, to your satisfaction you have the right to complaint to the Information Regulator.

Physical Address: SALU Building, 316 Thabo Sehume Street, Pretoria

Email: [inforreg@justice.gov.za](mailto:inforreg@justice.gov.za) Website: <http://www.justice.gov.za/inforeg/index.html>

A. Particulars of Complainant	
Name & Surname	
Identity no	
Postal address	
Contact no	
Email address	
B. Details of Complaint	
C. Desired Outcome	
D. Signature Page	
Signature:	Date: