

TYGERBERG GESINSKERK

COMPLIANCE MANAGEMENT FRAMEWORK: PROTECTION OF PERSONAL INFORMATION ACT ACT 4 OF 2013 ("POPI")

Document Ref.	POPI-0.1
Version:	1.0
Dated:	29 June 2021

Table of Contents:

No.	Clause	Pages
1.	INTRODUCTION	3
2.	PURPOSE	4
3.	RELEVANT LAWS	4
4.	GOVERNANCE	4
5.	DUTIES WITHIN THE FRAMEWORK	4
6.	DOCUMENTATION / POLICIES	6
7.	OVERVIEW	6
8.	TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE COMPLIANCE	7

1. INTRODUCTION

- 1.1. The Organisation is committed to protecting the privacy and security of individuals' Personal Information, in compliance with the Protection of Personal Information Act, 4 of 2013 ("POPI").
- 1.2. In terms of POPI, every person or entity who processes Personal Information must ensure that its systems and infrastructure supports the eight conditions for lawful processing, namely:
 - 1.2.1. Accountability
 - 1.2.2. Processing Limitation
 - 1.2.3. Purpose Specification
 - 1.2.4. Further Processing Limitation
 - 1.2.5. Information Quality
 - 1.2.6. Openness
 - 1.2.7. Security Safeguards
 - 1.2.8. Data Subject Participation
- 1.3. To ensure that Personal Information in the Organisation's possession or under its control is processed lawfully, the Organisation will implement appropriate technical and organisational measures, with emphasis on cyber security.
- 1.4. It is further necessary to adopt policies and procedures in relation to the processing of Personal Information to ensure that data subjects understand how and why their information is being processed and know what their rights are in relation to their personal information.
- 1.5. In addition, the Organisation seeks to mitigate its internal and external data security risks and protect its reputation, through compliance with POPI.
- 1.6. This Framework aims to provide a practical plan for the Organisation to follow in order to achieve compliance. It is divided into 10 main steps which are further subdivided into activities which the Organisation will undertake under this Framework.
- 1.7. In order to ensure the success of this Framework, the Organisation will increase data privacy awareness within the organisation and embed a culture of privacy and confidentiality into its operations.
- 1.8. The Information Officer will ensure that the Organisation is accountable for the Personal Information within the Organisation's control or possession.
- 1.9. The Organisation recognises that compliance is not a "once-off" activity and accordingly pledges its continued support to the ongoing implementation and development of this Framework.

- 1.10. Section 8 and 109(3)(g) of the Protection of Personal Information Act, 4 of 2013 (POPI) and Regulation 4(1)(a) of POPI requires Information Officers of public and private bodies to develop, implement, monitor and maintain a compliance framework which sets out the activities which the body intends to undertake in order to meet its ongoing compliance requirements under POPI.

2. PURPOSE

The purpose of this Framework is for the Organisation to:

- 2.1. Identify the accountability roles and individual responsibilities within the Framework;
- 2.2. Adopt a policy development and alignment plan;
- 2.3. Outline a policy implementation and execution strategy;
- 2.4. Detail the Organisation's approach to risk assessments; and
- 2.5. Describe the Organisation's approach to compliance monitoring.

3. RELEVANT LAWS

This Framework is aimed at compliance with the following laws:

- 3.1. Protection of Personal Information Act, 4 of 2013 (POPI);
- 3.2. Regulations relating to the Protection of Personal Information under (POPI); and
- 3.3. Guidance Notes issued by the Information Regulator in relation to POPI.

4. GOVERNANCE

4.1.	Information Officer	Riaan Daniël le Roux
------	----------------------------	----------------------

5. DUTIES WITHIN THE FRAMEWORK

- 5.1. The Information Officer is responsible for:
 - 5.1.1. To develop, implement, monitor and maintain this Compliance Framework;
 - 5.1.2. Ensuring that the Organisation abides by this Framework;
 - 5.1.3. Approving the compliance documentation;
 - 5.1.4. Implementing organisational and technological safety and security measures for the Organisation to safeguard Personal Information;
 - 5.1.5. Overseeing the procedures for a Data Subject's rights in terms of POPI and PAIA.
 - 5.1.6. Carrying out a Personal Information impact assessment when necessary to ensure the efficacy of security measures;
 - 5.1.7. To develop, monitor and maintain a PAIA Manual and ensure that adequate systems are in place to accommodate data subject requests in terms thereof;

- 5.1.8. Develop internal measures and systems to process requests for requests under POPI, requests for access and complaints;
 - 5.1.9. To arrange internal awareness sessions and materials for staff;
 - 5.1.10. Encourage compliance with POPI in the Organisation by implementing a Privacy Policy;
 - 5.1.11. Deal with requests by Data Subjects in terms of POPI;
 - 5.1.12. Provide cooperation to the Information Regulator in relation to investigations under Chapter 6 of POPI;
 - 5.1.13. Otherwise ensuring compliance by the Organisation with the provisions of POPI;
 - 5.1.14. To handle requests for copies of the PAIA Manual upon payment of the prescribed fee.
 - 5.1.15. Submit annual reports to the Information Regulator as contemplated in section 32 of PAIA.
- 5.2. All staff members (whether permanent, temporary, part-time or contract and including volunteers providing services to the Organisation) are responsible for:
- 5.2.1. Adhering to the following policies/processes of the Organisation:
 - 5.2.1.1. Privacy (POPI) Policy;
 - 5.2.1.2. POPI/PAIA Manual;
 - 5.2.1.3. Policy on Document Retention;
 - 5.2.1.4. Data Breach Management Policy;
 - 5.2.1.5. Employee consent and confidentiality clause;
 - 5.2.1.6. ICT Policy;
 - 5.2.1.7. Privacy Notice and Data Subject Consent.
 - 5.2.2. Attending compulsory POPI training from time to time;
 - 5.2.3. Reporting incidents of non-compliance with Policies to management.

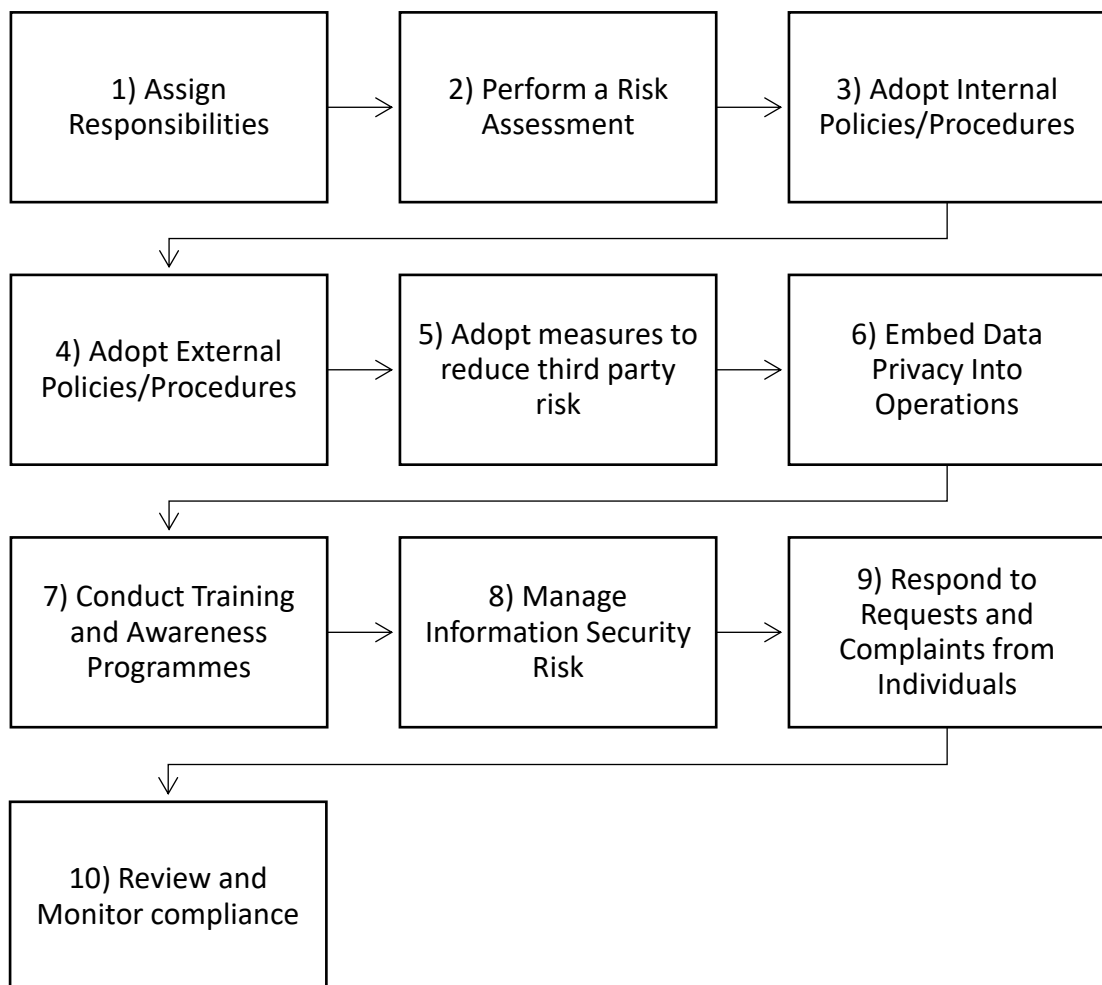
6. DOCUMENTATION / POLICIES

The Organisation will adopt the following documentation/policies to promote compliance with POPI:

Privacy Policy
PAIA/POPI Manual
Document Management Policy
Data Breach Management Policy
Employee consent and confidentiality clause
POPI clause for agreements
ICT Policy
POPI notice and Data Subject Consent Form
Personal Information Impact Assessment
POPI Compliance checklist
POPI clause for employment agreement

7. OVERVIEW

The structure of this Framework is based on the following 10 steps:



8. TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE COMPLIANCE

The following table sets out the activities and measures which the Organisation intends to undertake in order to achieve compliance with POPI:

ACTIVITY	TECHNICAL AND ORGANISATIONAL MEASURES	DOCUMENT	POPI SECTION REFERENCE	DUE DATE FOR COMPLETION
1. Assign Responsibilities	Appoint an Information Officer	<ul style="list-style-type: none"> Written Resolution of the Board of Directors Annexure A, B and C of the Information Regulator's Guidance Note on Information Officer, and Register the Information Officer with the Information Regulator on the electronic portal https://justice.gov.za/inforeg/portal.html 	55, 56 and Reg. 4	30 June 2021
	Determine the scope of the Information Officer's duties	<ul style="list-style-type: none"> Privacy Policy PAIA/POPI Manual 	55, 56 and Reg. 4	30 June 2021
	Assign responsibility for data privacy throughout the organization (incorporate into employment contracts and policies)	<ul style="list-style-type: none"> Contracts of Employment (job description) Privacy Policy PAIA/POPI Manual 	8	30 June 2021

	<p>Schedule a kick-off meeting with senior management to:</p> <ul style="list-style-type: none">• Give them information about POPI and the importance of privacy compliance; and• Determine, in broad terms, the most important focus areas/risks for your organisation.		8, 9, 19	30 June 2021
--	---	--	----------	--------------

<p>2. Perform a Risk Assessment</p>	<p>Carry out a Personal Information Impact Assessment:</p> <ul style="list-style-type: none"> • Compile an inventory of personal information currently being possessed or processed by the Organisation; • Record the current processing activities being undertaken by the Organisation in relation to personal information • Identify processors and review data processing agreements / Identify all agreements with third parties which involve the processing of personal information 	<p>Personal Data Impact Assessment Form Risk Assessment And Data Mapping</p>	<p>8, 10, 13, 17, 19, 20, 21 Reg. 4</p>	<p>30 June 2021</p>
--	---	--	---	---------------------

	<ul style="list-style-type: none"> • Identify all reasonably foreseeable internal and external risks to personal information under the Organisation's control or in its possession • For each type of processing operation, inventory the organisational and technical security measures you will take or have taken 			
	Complete a Gap Analysis	POPI Compliance Checklist	8, 19	30 June 2021
3. Adopt Internal Policies/procedures	Maintain a data privacy policy	POPI Policy		30 June 2021
	Circulate or publish an Employee Privacy Notice	Employee Privacy Notice		30 June 2021
	Insert a confidentiality clause into employment contracts	Confidentiality Clause for Contracts of Employment		30 June 2021

	Maintain a data breach management policy and a data breach register	Data Breach Management Policy		30 June 2021
	Adopt and implement a Records Retention and Disposal Policy	Records Retention and Disposal Policy		30 June 2021
	Adopt procedures for performing a Personal Information Impact Assessment before new processing activities are undertaken	Personal Information Impact Assessment		30 June 2021
4. Adopt external policies/procedures	Adopt a PAIA/POPIA Manual	PAIA/POPI Manual		30 June 2021
	Adopt a cookie policy	POPI Notice and Data Subject Consent Form		30 June 2021
	Adopt a Data Subject Consent Form	POPI Notice and Data Subject Consent Form		30 June 2021
	Adopt and make available forms for data subjects to exercise their rights under	PAIA/POPI Manual		30 June 2021

	POPI as prescribed in the Regulations to POPI			
	Update website terms and conditions in line with POPI	POPI Notice and Data Subject Consent Form		30 June 2021
	<p>Ensure that data subjects are informed of:</p> <ul style="list-style-type: none"> a) the fact that their data is being collected or processed, b) what information is being collected or processed, c) the purpose for which the information is being processed, d) the Organisation's name and address, e) whether the provision of the personal information 	POPI Notice and Data Subject Consent Form		30 June 2021

	<p>is compulsory or voluntary</p> <p>f) the consequences of failure to provide information</p> <p>g) any particular law authorising or requiring the collection of the information</p> <p>h) whether the information will be transferred to any third party or foreign country</p> <p>i) the source from which the information is collected (if not from the data subject directly)</p>			
--	---	--	--	--

	Adopt a personal information clause for contracts with Clients / Suppliers / Service Providers	Confidentiality Clause for Contracts		30 June 2021
	Maintain a data privacy notice	POPI Notice and Data Subject Consent Form		30 June 2021
5. Adopt measures to reduce third party risk	Maintain procedures to execute contracts or agreements with all operators/processors	Operator Agreement	19, 20, 21	30 June 2021
6. Embed Data Privacy Into Operations	Maintain policies/procedures for collection and use of Special Personal Information	Privacy Policy	26, 27, 28, 29, 30, 31, 32, 33	30 June 2021
	Maintain policies/procedures for collection and use of children and minors' personal data	Privacy Policy	34, 35	30 June 2021

	Maintain policies/procedures for maintaining data quality	Privacy Policy PAIA/POPI Manual	16	30 June 2021
	Maintain policies/procedures to review processing conducted wholly or partially by automated means	Privacy Policy	71	30 June 2021
	Maintain policies/procedures for further processing of personal data	Privacy Policy	15	30 June 2021
	Integrate data privacy into use of cookies and tracking mechanisms		5, 11	30 June 2021
	Integrate data privacy into direct marketing practices		5, 69	30 June 2021
	Integrate data privacy into e-mail marketing practices		5, 69	30 June 2021
	Integrate data privacy into telemarketing practices		5, 11	30 June 2021

	Integrate data privacy into digital advertising practices (e.g., online, mobile)		5, 11	30 June 2021
	Integrate data privacy into hiring practices		13	30 June 2021
	Integrate data privacy into the organization's use of social media practices		5, 11	30 June 2021
	Integrate data privacy into practices for monitoring employees		5, 8, 9, 11	30 June 2021
	Integrate data privacy into use of CCTV/video surveillance		5, 8, 9, 11	30 June 2021
	Integrate data privacy into delegate access to employees' Organisation e-mail accounts		8, 19	30 June 2021
7. Conduct Training and Awareness Programmes	Conduct privacy awareness training	Power Point Presentation	5, 8, 9, 11, 12, 13, 15	30 June 2021
	Conduct regular refresher training		8	1 December 2021

	Deliver a privacy newsletter to clients/service providers		8	30 June 2021
	Maintain privacy awareness material (e.g. posters and videos)	Posters X 2	8	30 June 2021
8. Manage Information Security Risk	Maintain technical security measures (e.g. encryption, intrusion detection, firewalls, monitoring)	POPI Policy	8, 19	30 June 2021
	Maintain procedures to restrict access to personal data (e.g. role-based access, segregation of duties)	POPI Policy	8, 19	30 June 2021
	Maintain an acceptable use of information resources policy	ITC Policy	8, 19	30 June 2021
9. Respond to Requests and Complaints from Individuals	Maintain procedures to address complaints	PAIA/POPI Manual Privacy Policy	5	30 June 2021
	Maintain procedures to respond to requests for access to personal data	Privacy Policy	5, 23	30 June 2021

	Maintain procedures to respond to requests and/or provide a mechanism for individuals to update or correct their personal data	Privacy Policy	5, 24	30 June 2021
	Maintain procedures to respond to requests to opt-out of, restrict or object to processing	Privacy Policy	5	30 June 2021
10. Review and Monitor compliance	Annual Personal Information Audit	Personal Data Impact Assessment Form Risk Assessment and Data Mapping		1 July 2022

THUS ACCEPTED AND SIGNED BY THE HEAD OF ORGANISATION AND INFORMATION OFFICER AT DURBANVILLE ON THIS THE 29TH DAY OF JUNE 2021



J L Delpont
Head of Organisation



R D le Roux
Information Officer





1.(POPI-1) POPI COMPLIANCE FRAMEWORK (for approval)

Final Audit Report

2021-06-29

Created:	2021-06-29
By:	Riaan le Roux (riaanle@gmail.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAAar5U6e0WP52asnJjO1PhVtYmymbLLX1E

"1.(POPI-1) POPI COMPLIANCE FRAMEWORK (for approval)" History

-  Document created by Riaan le Roux (riaanle@gmail.com)
2021-06-29 - 12:02:55 PM GMT- IP address: 8.35.59.38
-  Document emailed to Johannes Lodewikus Delport (johan@gesinskerk.co.za) for signature
2021-06-29 - 12:03:33 PM GMT
-  Email viewed by Johannes Lodewikus Delport (johan@gesinskerk.co.za)
2021-06-29 - 4:34:38 PM GMT- IP address: 105.184.248.159
-  Document e-signed by Johannes Lodewikus Delport (johan@gesinskerk.co.za)
Signature Date: 2021-06-29 - 4:35:08 PM GMT - Time Source: server- IP address: 105.184.248.159
-  Agreement completed.
2021-06-29 - 4:35:08 PM GMT