Telkom

Guideline

This guideline is intended to apply to Telkom SA SOC Limited and its Group of Companies

Protection of Personal Information Act 4 of 2013

POPIA Compliance Framework

Version: 1

TABLE OF CONTENT

DOCUMENT CONTROL INFORMATION

Document review and approvals		
Compiled by:	State the functional area (Group Finance), Section Name (Group Financial Control),	YYYY/MM/DD
	Name of Compiler and Signature	
Reviewed by:	Per the DOA, Policy Framework and approval matrix	YYYY/MM/DD
Approved by:	Per the DOA, Policy Framework and approval matrix	YYYY/MM/DD

Legal and Regulatory Service for Laws and Regulations impacting this document		
Reviewed by:	Legal Services	YYYY/MM/DD
Reviewed by:	Regulatory	YYYY/MM/DD

Quality Control					
Effective Date	This document comes into effect from	YYYY/MM/DD			
Type:	Group wide	Yes	√	No	
	Entity Specific - (Name of Entity)	Yes		No	√
	Division Specific - (Name of Division)	Yes		No	√
Risk Level	Procedure Review				
Level 1 – Group Wide	Every 3rd year **or** if there are any significant changes	Yes	√	No	
Level 2 – BU/Subsidiary	Every 3rd year **or** if there are any significant changes	Yes		No	√
Level 3 – Operational	Every 3rd year and no later than 5 years **or** if there are any significant changes	Yes		No	√
Level 4 - Other	In terms of legislative or business requirements	Yes		No	√
Saved by:	Group Financial Control	YYYY/MM/DD			

Version Control – Summary of Changes			
Version Number	**Paragraph**	**Description (changes since last version)**	**Date**
1	All	New document	YYYY/MM/DD

1 INTRODUCTION

As a responsible, forward-looking business, Telkom SA SOC Limited and its group of companies (hereafter "Telkom" or "the Organisation") recognises the need to comply with the Protection of Personal Information Act 4 of 2013 (POPIA) and ensure that effective measures are in place to protect personal information as guided by the POPIA.

The purpose of a compliance framework for the Protection of Personal Information Act is to establish, develop, implement, evaluate, maintain and improve an effective and responsive monitoring system within the context of the Organisation and its use of personal information.

A POPIA compliance framework is a requirement of the Regulations relating to the Act. It is the responsibility of the Information Officer (IO) to ensure that management, as responsible parties, implement a compliance framework.

2 APPLICABILITY AND SCOPE

This Compliance Framework applies to the Organisation as it endeavours to implement "appropriate technical and organisational measures" to secure the personal information they process. This can best be achieved via a formal framework structure for managing the security of personal information to be implemented in an integrated manner, and that can be evaluated and directed to ensure the rights to privacy of individuals in South Africa are protected.

The content of the compliance framework will differ depending on the size and level of maturity of the Organisation and on the context, nature and complexity of the Organisation's business activities. It should be based on the principles of good governance, proportionality, transparency and sustainability.

3 CONTEXTUAL BACKGROUND

A POPIA Compliance Framework for the protection of personal information will assist the Organisation to effectively and efficiently manage the compliance risks. The implementation thereof will support the aim of having an appropriate and consist of approach between external compliance requirements and internal policies, procedures, and regulations. The Organisation is to use the framework to establish a structured approach to continuously improve the various technical and complex requirements of the POPIA.

The development and implementation of a POPIA compliance framework provides for a commitment to the enablers of the protection for personal information and offers a monitoring capability to manage compliance with the obligations of the POPIA and ensure compliance with the conditions for the lawful processing of personal information.

The Information Regulator has extended the duties and responsibilities to ensure a suitable compliance framework is implemented. The Organisation, as a responsible party will have to demonstrate compliance to a wide range of legal obligations that include:

I. Keeping documentation that can be used later to demonstrate accountability.

II. Clarifying the roles, responsibilities and accountability obligations of responsible parties using risk-based approaches to data protection and the implementation of protective measures which correspond to the level of risk of processing personal information so that the fundamental rights and freedoms of data subjects are protected.

III. Supporting information officers and their efforts to achieve strong data protection compliance and establish effective privacy programmes.

IV. Providing effective governance of processors and third parties operating under the authority of the responsible party.

V. Pro-actively identifying and tracking procedural or training weaknesses in an effort to preclude regulatory violations.

4 RELEVANCE OF THE COMPLIANCE FRAMEWORK

The Organisation's recommended POPIA Compliance Framework consist of various Privacy Management Categories. Each category does have certain Technical and Organisational Measures which produce documentation (forms, policies, guidelines, etc.), that will help demonstrate ongoing compliance with the our POPI compliance obligations. As stated above, some activities may not apply to specific Business Units, Subsidiaries or sections.

The relevant POPI Act sections guiding the framework development include:

I. Section 8: The responsible party must ensure that the conditions set out in this Chapter, and all the measures that give effect to such conditions, are complied with at the time of the determination of the purpose and means of the processing and during the processing itself.

II. Section 109(3): When determining an appropriate fine, the Regulator must consider certain factors, including any failure operate good policies, procedures and practices to protect personal information.

III. Regulation 4(1)(a): An information officer must ensure that a compliance framework is developed, implemented, monitored and maintained.

The generic POPIA compliance framework addresses the eight conditions of lawful processing of personal information as encapsulated in the Act as well as the treatment thereof.

5 BENEFITS OF A POPIA COMPLIANCE FRAMEWORK

There are a number of reasons why the Organisation is required to have a compliance framework and monitoring system:

I. Being able to demonstrate commitment to compliance with the POPI Act, including the Regulations for the Protection of Personal Information, codes of conduct, binding corporate rules, organisational standards for data protection as well as standards of good corporate governance, best practices, ethics and data subject expectations.

II. Being able to safeguard their integrity, and avoid or minimize non-compliance with the Protection of Personal Information Act and its Regulations.

III. Being able to demonstrate socially responsible behaviour.

The compliance framework preserves a culture of respect for individual rights and the South African Constitution. Compliance with the POPIA is made sustainable by embedding it in a culture, behaviour and attitude of the people working for the Organisation. It is important that the compliance framework and monitoring system is part of, and integrated with, the Organisation's processes and overall management structure and that compliance is considered in the design of:

I. Organisational processes.

II. Information systems.

III. Internal controls.

It is expected that the compliance framework and monitoring system implementation will be scaled in accordance with the needs of the Organisation. The POPIA requirements are technical and complex and its implementation should be crafted for the specific needs of the Organisation's data subjects.

POPIA requires a process approach for establishing, developing, implementing, evaluating, maintaining and improving an effective and responsive compliance framework within the Organisation. Every organisation needs to identify and manage many activities related to the processing of personal information in order to function effectively, therefore a process approach is adopted to understand and accurately assess the impact of the processing of personal information on the affected data subjects.

6 POPIA COMPLIANCE FRAMEWORK SUPPORTING DOCUMENTS

To assist the Information Officer who is responsible for creating a POPIA Compliance Framework for the Organisation in addressing the requirement in terms of paragraph 4(1)(a) of the POPIA Regulations, Annexure B contains an extensive list of recommended documents that should aid the Organisation further in addressing the POPIA requirements, which may also already be incorporated in other existing internal documents.

In addition, Annexure C contains a high-level checklist that management can use to determine their function's readiness for compliance with the POPIA.

7 CONTACT DETAILS

Telkom has designated the undermentioned as our Information Officer/Deputy Information Officers with the responsibility to maintain our compliance with the POPI Act.

If you have any questions about our POPIA compliance framework, please contact us by email at popi@telkom.co.za

Contact details	
Information Officer	Sipho Maseko
Deputy Information Officers	Serame Taukobong, Consumer Althon Beukes, Openserve Lunga Siyo, Telkom Business Dirk Reyneke, Group Finance Melody Lekota, Group Human Resources
E-Mail Address	popi@telkom.co.za

Contact details	
	paia@telkom.co.za
Physical Address	The Information Officer 61 Oak Avenue Highveld, Technopark Centurion 0157
Postal address	Private Bag X881 Pretoria 0001
Information Regulator	
You have the right to lodge a complaint with the Information Regulator in writing as per their website https://www.justice.gov.za/inforeg/contact.html to:	
E-mail	**Complaints** email: complaints.IR@justice.gov.za **General enquiries** email: inforeg@justice.gov.za
Physical address	House 27 Stiemens Street Braamfontein Johannesburg 2001
Postal address	PO Box 31533 Braamfontein Johannesburg 2107

8 ENFORCEMENT AND VIOLATION

Compliance to this guideline will be monitored on a regular basis and the results reviewed by designated forums. Any breach will be treated as a serious disciplinary offence and may be subject to disciplinary in accordance with the provisions of the relevant Group HR policy.

9 DEFINITIONS, ABBREVIATIONS AND ACRONYMS

For definitions, acronyms and abbreviations refer to Annexure A of this document.

10 ANNEXURE A: DEFINITIONS, ACRONYMS, REFERENCE DOCUMENTS, LAWS & REGULATIONS

10.1 Definitions

Definitions	**Description**
Information Regulator	The Information Regulator (South Africa) is an independent body established in terms of section 39 of the Protection of Personal Information Act 4 of 2013. It is subject only to the law and the Constitution and it is accountable to the National Assembly.
Information Officer	POPIA Section 1 the Information Officer: "Of, or in relation to, a: (a) public body means an information officer or deputy information officer as contemplated in terms of section 1 or 17; or (b) private body means the head of a private body as contemplated in section 1, of the Promotion of Access to Information Act."
Deputy Information Officer	POPIA Section 56 states: "Designation and delegation of deputy information officers: Each public and private body must make provision, in the manner prescribed in section 17 of the Promotion of Access to Information Act, with the necessary changes, for the designation of: (a) such a number of persons, if any, as deputy information officers as is necessary to perform the duties and responsibilities as set out in section 55(1) of this Act; and (b) any power or duty conferred or imposed on an information officer by this Act to a deputy information officer of that public or private body."
Organisation	Telkom SA SOC Limited (group of companies, including all business units and subsidiaries)
Responsible party	POPIA Section 1 defines the role as follows: '''responsible party'' means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information".

10.2 Acronyms

Acronyms and Abbreviations	**Description**
POPIA	Protection of Personal Information Act 4 of 2013
PAIA	Promotion of Access to Information Act 2 of 2000
Telkom	Telkom SA SOC Limited (including business units and subsidiaries)

Acronyms and Abbreviations	Description
e.g.	Example

10.3 Reference Documents

I. POPIA Compliance Framework

10.4 Laws and Regulations

I. Protection of Personal Information Act 4 of 2013

II. GNR.1383 of 14 December 2018, Information Regulator: Regulations relating to the protection of personal information

III. Promotion of Access to Information Act 2 of 2000

IV. GNR.1244 of 22 September 2003 (which amended GNR.187 of 15 February 2002): Regulation of the Promotion of Access to Information Act 2 of 2000

V. GNR.1284of 4 October 2019, Rules of Procedure for Application to the court in terms of the Promotion of Access to Information Act 2 of 2000.

VI. All other laws, regulations, codes and standards relevant to Telkom.

11 ANNEXURE B: DETAIL POPIA COMPLIANCE FRAMEWORK EXAMPLE

The example of a generic POPIA compliance framework below, contains a list of both recommended and mandatory documents the Organisation should consider developing.

POPIA requires a process approach for establishing, developing, implementing, evaluating, maintaining and improving an effective and responsive compliance framework within the Organisation. Every organisation needs to identify and manage many activities related to the processing of personal information in order to function effectively, therefore a process approach is adopted to understand and accurately assess the impact of the processing of personal information on the affected data subjects.

_Compliance Statement				
Activity No	Activity	Template	Main POPIA Reference	Type
00.0	Create_Compliance Statement	_Compliance Statement		Optional

0 – Documentation Management				
Activity No	Activity	Template	Main POPIA Reference	Type
00.0	Create Summary 0 – Documentation Management	00.0_Summary Category 0_00_Documentation Management		Optional
00.1	Create Summary POPIA Compliance Framework	00.1_Summary POPIA Compliance Framework	**POPIA:** Section 8 & 109(3)(g) Regulations: R. 4(1)(a)	Mandatory
00.2	Create a Document Retention and Destruction Policy	00.2_Document Retention and Destruction Policy.	**POPIA:** Section 14 & 109(3)(g)	Mandatory
00.3	Create a Personal Information Assets Information Classification Matrix and Handling Guide	00.3_Personal Information Assets Information Classification Matrix and Handling Guide	**POPIA:** Section 109(3)(g)	Recommended
00.4	Create an Archiving of Records Register [To keep record of documents in archive]	00.4_Archiving of Records Register	**POPIA:** Section 14 & 109(3)(g)	Mandatory

0 – Documentation Management

Activity No	Activity	Template	Main POPIA Reference	Type
00.5	Create a Record Disposal Certificate [To keep record of disposed documents]	00.5_Record Disposal Certificate	**POPIA:** Section 14 & 109(3)(g)	Recommended
00.6	**Create a Records Disposal** Register [To keep record of disposed documents]	00.6_Records Disposal Register	**POPIA:** Section 14 & 109(3)(g)	Recommended
00.7	Develop & Implement a Register of Processing Documentation	00.7_Section 17 Register of Processing Documentation	**POPIA:** Section 8 & 17 Regulation:	Mandatory
	Additional Resource	Presentation: POPIA Awareness4_Security Measures in the Context of POPI - Leadership		

1 – Preparation for the Project

Activity No	Activity	Template	Main POPIA Reference	Type
01.0	Create Summary 1 – Preparation for the Project	01.0_Summary Category 01.0 – Preparation for the Project		Optional
01.2	Develop a POPIA Personal Information Impact Assessment and do an Assessment.	01.2_POPIA Personal Information Impact Assessment	**POPIA:** Section 8, 19 & 109(3)(g) **Regulation:** R. 4(1)(d)	Mandatory
01.4	Draw up an executive letter form the head of the Organisation to show to the staff, outside contractors that the top management support the implementation of a POPI Compliance Framework for the Organisation.	01.4_POPIA Executive Support Letter	**POPIA:** Section 8 **Regulation:** R. 4(1)(e)	Mandatory

1 – Preparation for the Project				
Activity No	Activity	Template	Main POPIA Reference	Type
01.5	Draw up a cover letter for Staff Members Knowledge Questionnaire	01.5_Project Cover letter for Staff Members Knowledge Questionnaire	**POPIA:** Section 8 **Regulation:** R. 4(1)(e)	Mandatory
01.6	Develop a start questionnaire to determine staff members knowledge	01.6_Project Start Questionnaire Staff Members Knowledge	**POPIA:** Section 8 Regulation: R. 4(1)(e)	Recommended
01.7	Draw up a cover letter for Leadership Knowledge Questionnaire	01.7_Project Cover letter for Leadership Knowledge Questionnaire	**POPIA:** Section 8 **Regulation:** R. 4(1)(e)	Recommended
01.8	Develop a start questionnaire to determine leadership knowledge	01.8_Project Start Questionnaire Leadership Knowledge Questions	**POPIA:** Section 8 Regulation: R. 4(1)(e)	
01.9	Develop a checklist to determining the data protection designation of the organisation	01.9_Determining the Data Protection Designation of the Organisation	**POPIA:** Section 1	
	Additional Resource	12.1.2_Checklist_Staff Awareness Training 12.2.2_Guideline Are you a Responsible Party or an Operator		

3 – 02_Implement & Maintain Governance & Leadership Structure				
Activity No	Activity	Template	Main POPIA Reference	Type
02.0	Create Summary Implement & Maintain Governance & Leadership Structure	02_Implement & Maintain Governance & Leadership Structure		
02.1	Develop and implement a Personal Information Protection Policy.	02.1_Personal Information Protection Policy	**POPIA:** Section 8 & 109(3)(g)	Mandatory

3 – 02_Implement & Maintain Governance & Leadership Structure				
Activity No	Activity	Template	Main POPIA Reference	Type
			Regulations: R. 4(1)(d)	
02.2	Draw up an appointment letter for the Information Officer	02.2_Appointment Letter Information Officer	**POPIA:** Section 55(1), 55(2) **PAIA:** Section 17, 90(1), 90(2), 90(3) & 77K POPIA Regulation: R. 4	Mandatory
02.3	Draw up a letter for the Authorisation of an Information Officer	02.3_Authorisation Letter Information Officer	**POPIA:** Section 55(1), 55(2) **PAIA:** Section 17, 90(1), 90(2), 90(3) & 77K POPIA Regulation: R. 4	Optional
02.4	Draw up an appointment letter for the Deputy Information Officer	02.4_Designation Letter Deputy Information Officer	**POPIA:** Section 55(1), 55(2) **PAIA:** Section 17, 90(1), 90(2), 90(3) & 77K POPIA Regulation: R. 4	Optional
02.5	Develop, draw up and get signed an addendum to employee's current service agreements	02.5_Access and Confidentiality Agreement with Employees	**POPIA:** Section 5 Regulation:	Mandatory
02.6	Develop Letter to Employees Privacy Notification	02.6_Letter to Employees Privacy Notification	**POPIA:** Section 18	Recommended
02.7	Develop POPIA Section 18 Privacy Notification - Employees	02.7_POPIA Section 18 Privacy Notification – Employees	**POPIA:** Section 18	Recommended
	Additional Resource	12.1.4_Checklist Section 17 - Documentation of processing operations		

3 – 02_Implement & Maintain Governance & Leadership Structure

Activity No	Activity	Template	Main POPIA Reference	Type
		12.2.4_Guideline Documentation Processing Operations		

4 - 03_Data Subject Rights

Activity No	Activity	Template	Main POPIA Reference	Type
03.0	03.0_Summary 03_Data Subject Rights Policies & Procedure			
03.1	Create Procedure for Handling of Individual Rights	03.1_Procedure for Handling of Individual Rights	**POPIA:** Section 5 & 109(3)(g) **Regulations:** Regulation 4(1)(d)	Mandatory
03.2	Create Consent for Processing of Personal Information	03.2_Consent to Process Personal Information Policy	**POPIA:** Section 14(7) **Regulations:** Regulation 4(1)(d)	Mandatory
03.3	Develop & implement privacy notification for clients	03.3_POPI Section 18 Privacy Notification - Clients	**POPIA:** Section 18	Mandatory
03.6	Create Data Subject Request Register	03.6_ Data Subject Request Register	**POPIA:** Section 14(7) **Regulations:** Regulation 4(1)(d)	Recommended
03.7	Create Forms and Procedure for Objection to the Processing of Personal Information	03.7_Form 1 Objection to the Processing of Personal Information	**POPIA:** Section 11(3) **Regulations:** Regulation 2	Mandatory
03.8	Create Forms and Procedure Request for Correction or Deletion of Personal Information	03.8_Form 2 Request for Correction or Deletion of Personal Information or Destroying or Deletion of	**POPIA:** Section 24(1) **Regulations:** Regulation 3	Mandatory

4 - 03_Data Subject Rights				
Activity No	Activity	Template	Main POPIA Reference	Type
	or Destroying or Deletion of Record of Personal Information	Record of Personal Information		
03.9	Create Forms and Procedure Request for Access to Record of Private Body	03.9_Form C Request for Access to Record of Private Body	**PAIA:** Section 51(1)(b)(iv) & 51(1)(e) **Regulations:** Regulation 10	Mandatory
03.10	Create Forms & Procedures for Withdrawal of Consent	03.10_Withdrawal of Consent	**POPIA:** Section 11(2)(b))	Recommended
	Additional Resource	12.1.5_Checklist Data Subject Rights Forms & Procedures 12.2.5_Guideline Data Subject Rights		

04_Implement & Maintain Personal Information Inventory				
Activity No	Activity	Template	Main POPIA Reference	Mandatory
04.1	Read How to find computer hardware	04.1_How to find computer hardware		Recommended
04.2	Create & Maintain Personal Information Assets Hardware	04.2_Personal Information Assets Hardware	**POPIA:** Section 8 & 109(3)(g) Regulations: R. 4(1)(d)	Recommended
04.3	Create & Maintain Personal Information Assets Shared Databases	04.3_Personal Information Assets Shared Databases	**POPIA:** Section 8 & 109(3)(g) Regulations: R. 4(1)(d)	Recommended
04.4	Create & Maintain Personal Information Assets Operating Systems and Software	04.4_Personal Information Assets Operating Systems and Software	**POPIA:** Section 8 & 109(3)(g) Regulations: R. 4(1)(d)	Recommended
	Additional Resource	04.1_How to find computer hardware		

05_Create & Maintain Policies & Procedures				
Activity No	Activity	Template	Main POPIA Reference	Type
05.0	05.0_Summary Create & Maintain Policies & Procedures			
05.1	Create & Implement Information Quality Policy	05.1_ Information Quality Policy	**POPIA:** Section 8 & 109(3)(g) Regulations: R. 4(1)(d)	Recommended
05.2	Create & Implement Minimum Access Policy	05.2_Minimun Access Policy	**POPIA:** Section 8 & 109(3)(g) Regulations: R. 4(1)(d)	Recommended
05.3	Create & Implement Password Management Policy	05.3_Password Management Policy	**POPIA:** Section 8 & 109(3)(g) Regulations: R. 4(1)(d)	Recommended
05.4	Create & Implement Acceptable Use Policy of Computer Equipment	05.4_ Acceptable Use Policy of Computer Equipment	**POPIA:** Section 8 & 109(3)(g) Regulations: R. 4(1)(d)	Recommended
05.5	Create & Implement Social Media Policy	05.5_Social Media Policy	**POPIA:** Section 8 & 109(3)(g) Regulations: R. 4(1)(d)	Recommended
05.6	Create & Implement Bring your Own Device Policy	05.6_Bring your Own Device Policy	**POPIA:** Section 8 & 109(3)(g) Regulations: R. 4(1)(d)	Recommended
05.7	Create & Implement Clear Desk and Clear Screen Policy	05.7_Clear Desk and Clear Screen Policy	**POPIA:** Section 8 & 109(3)(g) Regulations: R. 4(1)(d)	Recommended
05.8	Create & Implement Shred-it All Policy	05.8_Shred-it All Policy	**POPIA:** Section 8 & 109(3)(g)	Recommended

05_Create & Maintain Policies & Procedures				
Activity No	Activity	Template	Main POPIA Reference	Type
			Regulations: R. 4(1)(d)	
05.10	Create & Implement Removable Media Policy	05.10_Removable Media Policy	**POPIA:** Section 8 & 109(3)(g) Regulations: R. 4(1)(d)	Recommended
	Additional Resource	12.2.1_Guideline Cybersecurity Practices for Small Organisations		

06_Implement & Maintain Training & Awareness Program				
Activity No	Activity	Template	Main POPIA Reference	Type
06.0	06.0_Summary Implement & Maintain Training & Awareness Program			
06.1	Employee Training Log	06.1_Employee Training Log	**POPIA:** Section 8 Regulations: R. 4(1)(e)	Recommended
06.2	Employee Training Programme	06.2_Employee Training Programme	**POPIA:** Section 8 Regulations: R. 4(1)(e)	Recommended
06.3	Awareness Poster - Email Phishing	Awareness Poster - Email Phishing	**POPIA:** Section 8 Regulations: R. 4(1)(e)	Recommended
06.4	Awareness Poster - Insider, Accidental or Intentional Data Loss	Awareness Poster - Insider, Accidental or Intentional Data Loss	**POPIA:** Section 8 Regulations: R. 4(1)(e)	Recommended

06_Implement & Maintain Training & Awareness Program				
Activity No	Activity	Template	Main POPIA Reference	Type
06.5	Awareness Poster - Loss or Theft of Equipment and Data	Awareness Poster - Loss or Theft of Equipment and Data	**POPIA:** Section 8 Regulations: R. 4(1)(e)	Recommended
06.6	Awareness Poster - Make secure choices	Awareness Poster - Make secure choices	**POPIA:** Section 8 Regulations: R. 4(1)(e)	Recommended
06.7	Awareness Poster - What is my responsibility regarding e-mail security	Awareness Poster - What is my responsibility regarding e-mail security	**POPIA:** Section 8 Regulations: R. 4(1)(e)	Recommended
06.8	Awareness Poster - What is my responsibility regarding passwords	Awareness Poster - What is my responsibility regarding passwords	**POPIA:** Section 8 Regulations: R. 4(1)(e)	Recommended
06.10	Awareness Poster - What is our client’s (data subject) rights	Awareness Poster - What is our client’s (data subject) rights	**POPIA:** Section 8 Regulations: R. 4(1)(e)	Recommended
06.11	Awareness Poster - What is our legal basis for processing personal information	Awareness Poster - What is our legal basis for processing personal information	**POPIA:** Section 8 Regulations: R. 4(1)(e)	Recommended
06.12	Awareness Poster - What is Personal Information	Awareness Poster - What is Personal Information	**POPIA:** Section 8 Regulations: R. 4(1)(e)	Recommended
06.13	Awareness Poster - What to do when Using a Mobile Device	Awareness Poster - What to do when Using a Mobile Device	**POPIA:** Section 8 Regulations: R. 4(1)(e)	Recommended
06.14	POPI Act Compliance Awareness Poster	POPI Act Compliance Awareness Poster	**POPIA:** Section 8	Recommended

06_Implement & Maintain Training & Awareness Program				
Activity No	Activity	Template	Main POPIA Reference	Type
			Regulations: R. 4(1)(e)	
06.15	POPI Awareness1_An Overview Leadership	POPI Awareness1_An Overview Leadership	**POPIA:** Section 8 Regulations: R. 4(1)(e)	Recommended
06.16	POPI Awareness2_An Overview All Staff	POPI Awareness2_An Overview All Staff	**POPIA:** Section 8 Regulations: R. 4(1)(e)	Recommended
06.17	POPI Awareness3_Mobile Devices All Staff	POPI Awareness3_Mobile Devices All Staff	**POPIA:** Section 8 Regulations: R. 4(1)(e)	Recommended
06.18	POPI Awareness3_Mobile Devices All Staff	POPI Awareness4_Security Measures in the Context of POPI - Leadership	**POPIA:** Section 8 Regulations: R. 4(1)(e)	Recommended
06.19	POPI Awareness5_Collection of Personal Information in the Context of POPI - All Staff	POPI Awareness5_Collection of Personal Information in the Context of POPI - All Staff	**POPIA:** Section 8 Regulations: R. 4(1)(e)	Recommended
06.20	POPI Awareness6_Data Subject Rights - All Staff	POPI Awareness6_Data Subject Rights - All Staff	**POPIA:** Section 8 Regulations: R. 4(1)(e)	Recommended
06.21	POPI Awareness7_Electronic Communications - All Staff	POPI Awareness7_Electronic Communications - All Staff	**POPIA:** Section 8 Regulations: R. 4(1)(e)	Recommended
	Additional Resource	12.1.2_Checklist_Staff Awareness Training		

07_Manage Information Security Risk during Communication & Transmission				
Activity No	Activity	Template	Main POPIA Reference	Type
07.0	07.0_Summary Manage Information Security Risk during Communication and Transmission			
07.2	Create & implement Consent to Use Electronic Communication	07.2_Consent to Use Electronic Communication	**POPIA:** Section 8 & 109(3)(g) Regulations: R. 4(1)(d)	Recommended
07.3	Create & implement Fax Cover Letter Confidentiality Notice and Disclaimer	07.3_Fax Cover Letter Confidentiality Notice and Disclaimer	**POPIA:** Section 8 & 109(3)(g) Regulations: R. 4(1)(d)	Recommended
07.4	Create & implement Disclaimer Clauses for all Electronic Communications	07.4_Disclaimer Clauses for all Electronic Communications	**POPIA:** Section 8 & 109(3)(g) Regulations: R. 4(1)(d)	Recommended
	Additional Resource	12.2.1_Guideline Cybersecurity Practices for Small Health Care Organisations		

08_Third Party - Operator - Compliance Management				
Activity No	Activity	Template	Main POPIA Reference	Type
08.0	08.0_Summary Managing Third Party Compliance			
08.1	Create and maintain an Approved Vendors/Operator's list	08.1_ Approved Vendors/Operators	**POPIA:** Section 20, 21 & 22 Regulations: R. 4(1)(d)	Recommended
08.2	Create and prepare a Cover Letter to send with	08.2_Cover Letter Operator POPI	**POPIA:** Section 20, 21 & 22	Recommended

08_Third Party - Operator - Compliance Management				
Activity No	Activity	Template	Main POPIA Reference	Type
	Operator POPI Compliance Questionnaire	Compliance Questionnaire	Regulations: R. 4(1)(d)	
08.3	Create and prepare an Operator POPI Compliance Questionnaire	08.3_Operator POPI Compliance Questionnaire	**POPIA:** Section 20, 21 & 22 Regulations: R. 4(1)(d)	Mandated
08.4	Check all third-party service provider agreements and if necessary, implement this 08.5_ Data Protection Agreement for Operators	08.5_ Data Protection Agreement for Operators	**POPIA:** Section 20, 21 & 22 Regulations: R. 4(1)(d)	Mandated
	Additional Resource	12.2.3_Guideline Understanding whether you are Processing Personal Information		

09_Managing Direct Marketing				
Activity No	Activity	Template	Main POPIA Reference	Type
09.1	Create and maintain Application for the Consent of a Data Subject for the Processing of Personal Information	09.1_ Application for the Consent of a Data Subject for the Processing of Personal Information	**POPIA:** Section 69(2) Regulations: Regulation 6	Mandatory for direct marketing
	Additional Resource	12.2.3_Guideline Understanding whether you are Processing Personal Information		

10_Implement & Maintain Security Incident Procedures				
Activity No	Activity	Template	Main POPIA Reference	Type
10.0	10.0_Summary Implement & Maintain Security Incident Procedures			

10_Implement & Maintain Security Incident Procedures				
Activity No	Activity	Template	Main POPIA Reference	Type
10.1	Create and maintain Data Breach Policy Security Compromise Policy	10.1_Data Breach Policy Security Compromise Policy	**POPIA:** Section 8 Regulations: R. 4(1)(e)	Mandatory
10.2	Create and prepare 10.2_Data Breach Security Compromise Report Form	10.2_Data Breach Security Compromise Report Form	**POPIA:** Section 8 Regulations: R. 4(1)(e)	Mandatory

12 ANNEXURE C: POPIA HIGH-LEVEL CHECKLIST

Almost all organisations are faced with the challenge of achieving and maintaining compliance with the POPIA. This handy checklist provides a proven step-by-step forty-action-point approach to compliance.

12.1 Formalise your POPI Act compliance project

I. Identify your relevant stakeholders

II. Identify your project sponsor

III. Identify your project manager

IV. Set high level scope, timescale, budget

12.2 Appoint an Information Officer

I. Ensure alignment between your Promotion of Access to Information Act (PAIA) and POPI Information Officer (IO)

II. Decide whether the CEO can fulfil the IO function or needs a Deputy/Deputies (DIO)

III. Agree IO/DIO roles and responsibilities

IV. Complete the formal appointment process

12.3 Perform a gap analysis versus the POPI Act

I. Set interim and final targets for compliance with the POPIA. This does not mean slavishly shooting for 100% regardless of costs and benefits!

II. Engage with stakeholders in the assessment

III. Use an evidence-based approach

IV. Use the assessments for ongoing compliance monitoring

12.4 Analyse what and how Personal Information is processed

I. Use a broad definition of record types as per the POPIA (e.g. CCTV, biometric)

II. Look at various aspects as required by the POPIA (including consent, purpose, source, sharing, destruction)

III. Consider user rights and their management

IV. Think broadly in terms of the types of devices where data is stored – and represents a security compromise risk

12.5 Implement POPI Act compliance policies

I. Review existing relevant policies

II. Ensure your policies are reasonable and appropriate

III. Make sure your policies are enforceable

IV. Design your Privacy Notices for diverse stakeholder groups

12.6 Review your web sites

I. Develop your checklist of what to review

II. Agree the rating scheme to be used

III. Use the opportunity to implement “best practice” such as Cookie notifications

IV. Develop and implement your remediation plan

12.7 Update / create your PAIA manual

I. Confirm your organisation needs a Promotion of Access to Information Act (PAIA) manual and by when

II. Confirm whether you are a Public or Private Body as per the PAIA

III. Review the proposed contents of your manual

IV. Ensure your PAIA manual follows the prescribed layout and includes the necessary details

12.8 Implement the POPIA compliant PI management processes

I. Look at the PI lifecycle: including acquisition, processing, retention, and destruction practices

II. Develop reasonable and appropriate measures to ensure ongoing compliance

III. These could include self-assessments, health-checks, formal audits

IV. Develop your dashboard for compliance

12.9 Train stakeholders about their roles in POPIA compliance

I. Design training according to their needs

II. Ensure you treat user education not as a once-off series of activities but part of an ongoing commitment

III. Leverage diverse training methods, including self-study, online, classroom, audio and video

IV. Look to special needs such as the IO/DIO roles

12.10 Make the POPIA compliance “Business-As-Usual”

I. Recognise that POPIA compliance will be the “new normal” and work that way

II. Build compliance into your products, services and processes – adopt “Privacy-By-Design”

III. Ensure ongoing monitoring of the data protection / the POPIA ecosystem – legislation, regulations, opportunities and threats

IV. Build the POPIA into your everyday operations – make the POPIA “Business-As-Usual”

13 ANNEXURE D: APPROVALS

Sample - review and approvals