

**PROTECTION OF  
PERSONAL  
INFORMATION POLICY  
TT-FOA-22**

Standard Operating Policy – Finance,  
Operations & Administration

Effective Date



24 August 2021

## DOCUMENT CONTROL

### Document Information


Property	Description
Document Title	Conflict of Interest Policy
Document No.	TT-FOA-22
Document Author	Tshiamiso Trust Board
Change Date	21 October 2021
Active Date	24 August 2021

### Change Record

Date	Effective Date	Author	Version	Signature
31/07/2021		K Sedupane	2	
21/10/2021		T Mtshemla	3	

### Approvals

The signatures below confirm that the reviewers agree with the content of the document and that this document is approved for implementation within Tshiamiso Trust.

Name	Position	Signature	Date
Prof. May Hermanus	Chairperson: Board of Trustees		
Kgomotso Molebatsi	Chairperson: HR, Remuneration and Governance Committee		
Daniel Kotton	Chief Executive Officer		02/11/2021

This document is effective from the date of the last approval signature.

### Document Location

The original signed document is held by: The Trust  
When printed this document is uncontrolled

## CONTENTS

---

1. STATEMENT FROM THE TSHIAMISO TRUST TRUSTEES	5
2. INFORMATION PROCESSING TERMS AND DEFINITIONS	5
3. SCOPE AND APPLICATION	7
4. LAWFUL BASIS FOR PROCESSING	7
5. CONSENT	7
6. PURPOSE SPECIFIC	9
7. ACCURACY	10
8. DATA MINIMISATION	10
9. TRANSPARENCY AND PROCESSING NOTICES	11
10. CONFIDENTIALITY, INTEGRITY AND SECURITY OF PERSONAL INFORMATION	13
11. RECORDS MANAGEMENT: CLASSIFICATION	13
12. RECORDS MANAGEMENT: STORAGE	15
13. RECORDS MANAGEMENT: RETENTION AND DISPOSAL	18
14. OPERATORS	20
15. SHARING PERSONAL INFORMATION	20
16. CROSS BORDER TRANSFERS OF PERSONAL INFORMATION	21
17. REPORTING PERSONAL INFORMATION BREACHES	23
18. DATA SUBJECT RIGHTS AND REQUESTS	24
19. THE RIGHT TO COMPLAIN	25
20. GOVERNANCE	25
21. TRAINING	27
22. NON-COMPLIANCE	28

<b><u>ANNEXURE A</u></b>	<b>29</b>
<b>DOCUMENT CLASSIFICATION AND MANAGEMENT REGISTER FORMAT</b>	<b>29</b>
<b><u>ANNEXURE B</u></b>	<b>43</b>
<b>INCIDENT INVESTIGATION FORM</b>	<b>43</b>

## **1. STATEMENT FROM THE TSHIAMISO TRUST TRUSTEES**

- 1.1 Tshiamiso Trust is committed to conducting business with the highest level of integrity, in accordance with the highest ethical standards and in full compliance with all applicable laws, including the law known as the Protection of Personal Information Act, 4 of 2013, (POPIA), which regulates the Processing of Personal Information.
- 1.2 The Protection of Personal Information Policy has been developed at the direction of Tshiamiso Trust's Trustees in order to provide clear guidance to all employed and utilised by the Trust, and who Process Personal Information on how they are to Process Personal Information, thereby ensuring that all Personal Information Processed by the Trust is done in a lawful, transparent and consistent manner and in full compliance with all and any applicable data protection laws which may from time to time apply to its activities and operations, including POPIA and the General Data Protection Regulation 2016/679 (GDPR) applicable in the EU (hereinafter referred collectively as the "Data protection laws").
- 1.3 Tshiamiso Trust requires compliance with all its policies, including this Protection of Personal Information Policy.

## **2. INFORMATION PROCESSING TERMS AND DEFINITIONS**

POPIA makes use of certain terms and references, which will be used in this Policy, which are explained below:

- 2.1 **"Consent"** means in relation to POPIA, any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the Processing of Personal Information about them;
- 2.2 **"Data Subject"** means any individual or legal entity;
- 2.3 **"Operator"** means any person who Processes Personal Information on behalf of a Responsible Party as a contractor or sub-contractor, in terms of a contract or mandate, without coming under the direct authority of the Responsible Party;
- 2.4 **"Processing Notices"** means a notice setting out the prescribed information that must be provided to Data Subjects before collecting his, her or its Personal Information, (also known as "section 18 POPIA notices", "privacy notices" or "data protection notices").

- 2.5 **“Personal Information”** means Personal Information relating to any identifiable, living, natural person, and an identifiable, existing juristic person, including, but not limited to:
- name, address, contact details, date of birth, place of birth, identity number, passport number;
  - bank details;
  - qualifications, expertise, employment details;
  - tax number;
  - vehicle registration;
  - dietary preferences;
  - financial details including credit history;
  - next of kin / dependants;
  - education or employment history; and
  - **Special Personal Information**, being including race, gender, pregnancy, national, ethnic or social origin, colour, physical or mental health, disability, criminal history, including offences committed or alleged to have been committed, membership of a trade union and biometric information, such as images, fingerprints and voiceprints, blood typing, DNA analysis, retinal scanning and voice recognition.
- 2.6 **“Personnel”** means Tshiamiso Trust trustees, employees, committee members, executives and any other person who may Process Personal Information on behalf of the Tshiamiso Trust.
- 2.7 **“Processing, Process, Processed”** means in relation to Personal Information, the collection, receipt, recording, collation, storage, updating or modification, retrieval, alteration, consultation or use; dissemination by means of transmission, distribution or making available in any other form; merging, linking, as well as restriction, degradation, erasure or destruction of information; or sharing with, transfer and further Processing, including physical, manual and automatic and in relation thereto which may be held on a **“Record”** which means any recorded information housing Personal Information Processed by the Tshiamiso Trust, or its Personnel, regardless of form or medium.
- 2.8 **“Purpose”** means the underlying reason why a Responsible Party or Operator needs to Process a Data Subject’s Personal Information.
- 2.9 **“Responsible Party”** means, in relation to POPIA, the person or legal entity who is Processing a Data Subject’s Personal Information, in this case being the Tshiamiso Trust, and its Personnel.
- 2.10 **“Records”** means all documents and records housing data, including held, created, used or processed by Tshiamiso Trust, including Records containing Personal Information.

### 3. SCOPE AND APPLICATION

This Policy applies to any persons who Process Personal Information on behalf of Tshiamiso Trust, including Tshiamiso Trust trustees, executives, employees and Operators, who will hereinafter be referred to collectively as "Personnel".

### 4. LAWFUL BASIS FOR PROCESSING

In terms of POPIA, where Personal Information is Processed such Processing must be done lawfully and in a reasonable manner that does not infringe on the privacy of the Data Subject. In order to discharge the above obligations, Personnel must comply with the Processing guides, rules and procedures set out below.

### 5. CONSENT

5.1 A Data Subject does not have to Consent to the Processing of his, her or its Personal Information where there is a lawful basis for such Processing. A lawful basis for Processing in terms of the Data Processing laws, is where:

- the Processing is **necessary to conclude a contract** to which the Data Subject is a party and to perform contractual obligations or give effect to contractual rights;
- the Processing is necessary in order to **comply with a law** or to comply with certain legal obligations imposed by a law;
- the Processing is necessary to **protect Tshiamiso Trust's legitimate interests or rights, the Data Subject's legitimate interests or rights or a third party's legitimate interests or rights**, unless there is a good reason to protect the Data Subject's Personal Information which overrides those legitimate interests;
- the Processing is necessary in order to perform a **public duty** or to perform tasks carried out in the public interest or the exercise of official authority.

5.2 Where there is no lawful basis for the Processing, then the Data Subject, has to Consent to the Processing.

- 5.3 Personnel must ensure that prior to Processing a Data Subject's Personal Information, that there is either a lawful reason for the Processing, or alternatively that the Data Subject has Consented to such Processing, which lawful reason will be described under the specific and informative Tshiamiso Trust Processing notices, or in the absence of a lawful reason, will call for the Data Subject's consent.
- 5.4 A Data Subject may withdraw his, her, its Consent so long as it provides Tshiamiso Trust with a "withdrawal of consent notice", which notice is available on Tshiamiso Trust website, which request will be handled and actioned directly by the duly appointed Tshiamiso Trust Information Officer or Deputy Information Officer, (Information Officer), which outcome in turn, will be relayed to the respective Personnel who has been Processing such Personal Information.
- 5.5 A Data Subject may not withdraw Consent where no Consent is required, i.e., where Tshiamiso Trust can show that there is a lawful basis for the Processing. In such a case the Data Subject may only object to such Processing, provided that an "Objection notice" is sent to Tshiamiso Trust, which notice is available on Tshiamiso Trust website, which request will be handled and actioned directly by the Information Officer and which outcome will be relayed to the respective Personnel who has been Processing such Personal Information.
- 5.6 Where a Data Subject withdraws Consent or objects to the Processing, in such case Tshiamiso Trust and the respective Personnel who has been Processing the impacted Personal Information, will have to stop Processing the Personal Information, unless Tshiamiso Trust can show compelling legitimate grounds for the Processing which overrides the interests, rights and freedoms of the Data Subject, or the Processing is necessary for the establishment, exercise or defence of legal claims.
- 5.7 The Information Officer will at the time of the withdrawal or objection referred to above, explain to the Data Subject the effects and consequences of any withdrawal or objection and relay the outcome to the respective Personnel who has been Processing such Personal Information.



## **6. PURPOSE SPECIFIC**

### **6.1 Personal Information:**

- may only be collected for a specified, explicit and legitimate purpose;
- must only be used for the purpose for which it was collected and for no other purpose, unless the Data Subject has been informed of the other purposes;
- may not be further Processed or used for any subsequent purpose, unless that Personal Information is required for a similar purpose; and such Processing is compatible with the initial purpose.

### **6.2 Tshiamiso Trust for the purposes of carrying out its trust objectives and related operational and business objectives, Processes Personal Information belonging to a vast range of Data Subjects, including employees, its trustees, agents, committees and committee members, medical boards and panels, claimants, prospective employees and job applicants, students and interns, service providers and contractors, vendors, stakeholders, and other third parties, which Processing is required for a variety of trust and operational-related purposes.**

### **6.3 Examples of these purposes are described below:**

- to recruit and employ - employment;
- to recruit and appoint trustees, board members, agents, boards and panels;
- concluding and managing a contract or trust related transaction - contract;
- conducting criminal reference checks - legitimate interest;
- conducting medical examinations and assessments- legitimate interest;
- conduction risk assessments - legitimate interest;
- for insurance and underwriting purposes - legitimate interest;
- assessing and Processing claims, queries, enquiries, and complaints, - legitimate interest;
- conducting credit checks - legitimate interest;
- confirming, verifying and updating personal details - legitimate interest;
- detection and prevention of fraud, crime, money laundering or other malpractices - legitimate interest;
- conducting research - legitimate interest;
- audit and record keeping purposes - legitimate interest;
- budgeting, processing claims, paying beneficiaries, collecting contributions and managing debtor and creditors - legitimate interest;
- complying with laws and regulations - laws;
- dealing with medical experts, medical boards, and other regulators - laws;

- paying taxes - laws;
- collecting debts or legal proceedings - legitimate interest;
- communications - legitimate interest;
- managing employees and the trust activities, in order to comply with its mandate as per the Trust Deed - contractual and employment.

6.4 Tshiamiso Trust personnel must:

- ensure that before Personal Information is Processed, there is a valid and legitimate reason for such Processing; and
- advise all Data Subjects why the Personal Information is required, i.e., the purpose for the Processing, which purpose will be described under the Tshiamiso Trust Processing notices, housed on the Tshiamiso Trust website, which the Data Subject should be directed to.

## 7. **ACCURACY**

7.1 All Personal Information Processed by Tshiamiso Trust must be accurate and, where necessary, kept updated.

7.2 In order to ensure that Personal Information is accurate and is up to date, Personnel must:

- take all and every reasonable step to ensure that all Personal Information which they Process is accurate, having regard to the purposes for which it is Processed, and where it is found to be inaccurate, that it is where possible, updated and rectified without delay;
- implement procedures allowing Data Subjects to update their Personal Information;
- send out regular communications to Data Subject requesting “updates to details” which if responded to, should be acted on immediately by the relevant or responsible division, section or department;
- where appropriate, and possible, ensure that any inaccurate or out-of-date records are updated and the redundant information deleted or destroyed;
- take note of the rights of the Data Subject in relation to updates and rectifications of Personal Information, housed under the Tshiamiso Trust Processing Notices and give effect to any update request, when such request has been communicated through to it by the Information Officer.

## 8. **DATA MINIMISATION**

8.1 Tshiamiso Trust may not Process Personal Information which is not necessary for the Purpose for which the Personal Information is Processed.

8.2 Personnel must:

- ensure that when they process Personal Information on behalf of Tshiamiso Trust, that it is adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed; and
- revisit all pre-populated questionnaires and forms which are currently used to collect or house Personal Information and consider the purpose or reason for the collection and thereafter analyse the types of Personal Information which is request or collected and where of the view that certain Personal Information is not needed for the defined purpose, then such information should no longer be called for, collected and/or recorded and the relevant areas where this information is housed or asked for should be deleted.

## 9. TRANSPARENCY AND PROCESSING NOTICES

9.1 Tshiamiso Trust has a duty to show that it has dealt with a Data Subject in a transparent manner.

9.2 In order to demonstrate transparency, Tshiamiso Trust must refer all Data Subjects, to a specific and informed Processing Notice, at the time when Tshiamiso Trust collects and Processes a Data Subject's Personal Information or within a reasonable period thereafter, which Processing notice must set out:

- the types of Personal Information Processed, and the purpose or reason for the Processing;
- the lawful basis relied upon for such Processing or whether Consent is required for the Processing;
- the period for which the Personal Information will be retained;
- who the Personal Information will be shared with, including external or cross border transfers and the mechanism(s) relied upon for such transfer;
- the security measures which are in place to protect the Personal Information, including where the Personal Information is sent to parties cross border and the mechanism(s) relied upon for such protection; and
- the respective rights of the Data Subject and how these rights may be exercised.

9.3 In order to meet its obligations under 9.2 above, Tshiamiso Trust has developed and placed on its website the following informed and specific Processing Notices which apply to the different Data Subject categories with whom it deals with:

- a **Human Resources Processing Notice**, which applies to all employees – perspective and actual, all bursary or learnership beneficiaries - prospective or actual;
- a **Procurement Processing Notice**, which applies to all participants in Tshiamiso Trust supply chain, including persons who provide goods and services to Tshiamiso Trust (service providers), and/or other parties who Tshiamiso Trust

may engage with and who make up the Tshiamiso Trust procurement and supply chain, including Regulators;

- a **Company Secretarial Processing Notice**, which applies to all Data Subjects who deal with the Tshiamiso Trust from a company secretarial perspective, including trustees, Regulators, stakeholders and/or other parties who Tshiamiso Trust may engage with;
- a **Claimants and Trust Processing Notice**, which applies to all Data Subjects who deal with the Tshiamiso Trust from a claimant perspective;
- a **Security Processing Notice**, which applies to any persons who come onto Tshiamiso Trust sites, facilities and offices and who Tshiamiso Trust may engage with;
- a **Website Privacy Notice** which applies to any persons who make use of Tshiamiso Trust websites, social media websites, emails, and other IT related communications facilities and platforms.

9.4 In order to give effect to the above transparency requirement, Personnel:

- must all understand the provisions of the Data Processing laws;
- familiarise themselves with the abovementioned Tshiamiso Trust Processing Notices and any others which Tshiamiso Trust may implement from time to time, and any changes made thereto;
- familiarise themselves with, where applicable, Tshiamiso Trust standard binding corporate rules, its standard Personal Information transfer agreement and/or its Operator agreement;
- ensure that all Tshiamiso Trust documents, forms or other records (Records) which house or call for Personal Information contain the following Data Processing details:

**Please note that in order for Tshiamiso Trust to engage with you, it will have to Process certain Personal Information which belongs to you, which Processing is described and explained under the specific and informative Tshiamiso Trust Processing Notices, housed for ease of reference on the Tshiamiso Trust's website which we ask that you download and read. By providing us with the required Personal Information, such act will be taken as an indication that you have read and agree with the provisions described under the Processing Notice and where applicable, you consent to the processing by us of your Personal Information.**

- at the time of Processing, direct the Data Subjects who you deal with to the applicable area of Tshiamiso Trust website where the specific and informative Tshiamiso Trust Processing notices are housed.

## **10. GENERAL DUTIES: CONFIDENTIALITY, INTEGRITY AND SECURITY OF PERSONAL INFORMATION**

10.1 In order to safeguard, secure and ensure the confidentiality and integrity of all Personal Information held by or under the control of Tshiamiso Trust, the Tshiamiso Trust together with its Personnel must;

- identify all reasonably foreseeable internal and external risks to Personal Information in its possession or under its control;
- document the identified risks;
- establish, in response to the identified risks, reasonable technical and organizational measures across all areas where Personal Information is held or stored, including electronic and physical mediums;
- implement and maintain all approved and required measures across all areas where Personal Information is held or stored, including electronic and physical measures, all which are designed to minimise the risk of loss, damage, unauthorised destruction and/or unlawful access of Personal Information;
- regularly verify that these measures are effectively implemented; and ensure that the measures are continually updated in response to new risks or deficiencies in previously implemented measures and safeguards, which measures include, where appropriate, among others, the following:
  - the pseudonymisation and encryption of Personal Information;
  - ongoing efforts to ensure the long-term confidentiality, integrity, availability and resilience of Personal Information housed within the Tshiamiso Trust environment;
  - applications and processes which have the ability to rapidly restore the availability of and access to Personal Information in the event of a tangible or technical incident; and
  - procedures for the regular review, assessment and evaluation of the effectiveness of the technical and organizational measures taken to ensure the security of Processing, including regular IT Security Audits.

10.2 The duty to ensure data privacy, confidentiality and integrity of Personal Information starts when Tshiamiso Trust initially interacts with a Data Subject and will continue throughout the relationship, until the purpose for the Processing of the Personal Information comes to an end.

## **11. RECORDS MANAGEMENT DUTIES: CONFIDENTIALITY, INTEGRITY AND SECURITY OF PERSONAL INFORMATION**

11.1 In order to ensure the confidentiality and integrity of all Records, especially those which house or contain Personal Information which are held by Tshiamiso Trust, and in order to safeguard and secure these Records, Personnel must ensure that:

- 11.1.1 all Processing of Personal Information activities and communications are reduced to writing and retained in a Record, which Record may either be electronic, or paper based;
- 11.1.2 each Record created is classified, and then is housed in a folder (Folder), and where applicable in sub folders of the Folder being a storage area, either electronic or paper based and in turn each Folder / subfolder is given an appropriate title or Folder name using the Tshiamiso Trust naming convention and classification guide and template set out under **Annexure “A”**;
- 11.1.3 Folders and Records must be named in a consistent and logical manner so they can be located, identified and retrieved as quickly and easily as possible;
- 11.1.4 all Folders and Records must be stored and saved in a way that the contents are safeguarded and are identifiable as per the agreed Tshiamiso Trust naming convention and classification;
- 11.1.5 the name of the Folder and related sub folders and Records held in such Folders, together with the classification thereof must be recorded in a department specific records register which has to be compiled for each department, using Tshiamiso Trust standard department management register (hereinafter referred to as “the **“Department Records Management Register”**”), as set out under **Annexure “A”**, including the following details:
- classification;
  - the name of the Folder and related Records;
  - format of the Folder and related Records;
  - location of Record - including physical or electronic location;
  - who has access to the Folder, and the Records;
  - status of the Folder and the Records;
  - retention period pertaining to the Folder and/or Records; and
  - destruction date of the Records, when available;
- 11.1.6 their respective department head reviews their own department specific Department Records Management Register annually to ensure compliance with this Policy;
- 11.1.7 each department provides a copy of its Department Records Management Register to the Information Officer, annually, or on request.
- 11.2 Upon termination of employment, or change of job roles or responsibilities of Personnel, the affected line manager responsible for such Personnel must ensure that all access rights to any Tshiamiso Trust Folders or Records is removed immediately and that all Tshiamiso Trust assets used to access the Folders and or Records are returned to Tshiamiso Trust, and that all physical access rights to Tshiamiso Trust premises and facilities are revoked or cancelled.

## **12. RECORDS MANAGEMENT DUTIES: STORAGE OF RECORDS HOUSING PERSONAL INFORMATION**

12.1 In order to ensure the confidentiality and integrity of all paper-based Records which house or contain Personal Information, which are held by Tshiamiso Trust, and in order to safeguard and secure these Records, Personnel must ensure that all paper-based Records:

- which are housed in physical storage areas are labelled and the details recorded in the Department Management Register;
- when in use, are not left around for others to access, and are not left in places where persons can view the contents e.g., on a printer or on unmanned desks;
- are stored securely when not in use, in Folders, which in turn are placed in locked boxes, drawers, cabinets, or similar structures or containers;
- that only Personnel who are required, on an operational and need to know basis, are given access to such Records and/or Folders; and
- such Records and/or Folders are only removed from Tshiamiso Trust premises if such removal is recorded in the Department Records Management Register and when removed off site, such Records are safeguarded and kept confidential.

12.2 In order to ensure the confidentiality and integrity of all electronic Records which house or contain Personal Information, which are held by Tshiamiso Trust, and in order to safeguard and secure these Records, Personnel must ensure that:

- they comply with all applicable Tshiamiso Trust IT Policies and Procedures, especially Tshiamiso Trust IT end user policy;
- all electronic Records are stored and housed on Tshiamiso Trust servers which are protected by approved security software, and one or more firewalls under the direction of Tshiamiso Trust IT Manager and where transferred or uploaded to cloud computing services from computers, devices and applications, that these services have been approved by Tshiamiso Trust IT Manager;
- all devices where electronic Folders and/ or Records are stored, are password protected and that passwords are not written down or shared, irrespective of seniority or department, which passwords must be strong passwords which are changed regularly. If a password is forgotten, it must be reset using the applicable method;
- all network devices and drives where electronic Folders and Records are stored have access control measures in place;
- electronic Folders and Records are not stored on mobile devices and removable media, which includes, but is not limited to: smart phones, tablets and I pads, Digital media, USB sticks, external hard drives, CDs, DVDs, memory cards, tapes, unless the device is password protected and the content of such Record(s) is where possible encrypted;

- where one needs to use and access the contents of an electronic Folder or Record, off site, which will not be accessed using Tshiamiso Trust secured servers, and which will be downloaded on to portable device for off-site working purposes, such person must only remove the Folders and/or Records or parts thereof if such removal is recorded in the Department Records Register; only the record(s) which are necessary for one's immediate needs are removed; where possible and feasible, the Personal Information to be removed is strongly encrypted; and when removed off site, such Records are safeguarded and kept confidential and when no longer needed, that the removed Folder and/or Record, once dealt with is deleted from the portable device;
- all electronic Records are regularly backed up using Tshiamiso Trust provided systems and applications and in accordance with backup protocols. Such backups will be tested regularly in line with Tshiamiso Trust standard backup procedures and protocols under the direction of the IT Manager;
- all device screens, when not in use are always locked especially when left unattended and password protected;
- electronic Records are only transmitted over secure networks, including wireless and wired networks.

12.3 In order to ensure the confidentiality and integrity of all Records which house or contain Personal Information, which are held by Tshiamiso Trust, and in order to safeguard and secure these Records, Personnel must ensure that:

12.3.1 Records are shared with others on a “*need to know*” basis only. If Personnel are unclear on how to apply this requirement, the default position is that a conservative approach must be applied, i.e. information must be disclosed only to those people who have a legitimate business need for the information;

12.3.2 controls are in place to ensure that only personnel with proper authorization and a need to know are granted access to Tshiamiso Trust systems and resources. Remote access shall be controlled through identification and authentication mechanisms;

12.3.3 proper controls are in place to authenticate the identity of Personnel or any third party who needs to access a Record, and all Personnel validate each person who requires access to the Record before allowing them access;

12.3.4 data used for authentication shall be protected from unauthorized access;

12.3.5 access to information classified as Special Personal Information or sensitive Personal Information must be provided only after the written authorisation of the Data Owner has been obtained, under a Onwards transmission notice. In this regard Personnel must refer all requests for access to the relevant Data Owners or their delegates for permission and signature of the Onwards transmission notice.

12.3.6 special needs for other access privileges will be dealt with on a request-by-request basis;

12.3.7 storage media containing Special Personal Information or sensitive (i.e. restricted or confidential) information shall be completely empty before reassigning that medium to a different user or disposing of it when no longer used. Simply deleting the data from the media is not sufficient. A method must be used that completely erases all data. When disposing of media containing data that cannot be completely erased it must be destroyed in a manner approved by the IT department.



- 12.4 Any attempts to bypass security controls or to obtain unauthorised access, or to make unauthorised use of another's account shall be considered a security breach or violation.
- 12.5 The use of any Trust information or data for purposes other than for authorised Trust purposes shall be considered a security violation.
- 12.6 The use of any Trust information or data for any unauthorised or illegal activity shall be considered a security breach or violation.
- 12.7 Any act, or failure to act, that constitutes or causes a security incident or creates a security exposure shall be considered a security breach or violation.
- 12.8 Any act, or failure to act that results in sensitive or business critical information being disclosed to an unauthorised person shall be considered a security breach or violation.
- 12.9 Any act, or failure to act that results in sensitive or business critical information being modified or destroyed, such that Tshiamiso Trust is adversely impacted shall be considered a security breach or violation.
- 12.10 Any breach of this policy shall be considered a security breach or violation.

### **13. RECORDS MANAGEMENT DUTIES: RETENTION AND DISPOSAL OF RECORDS HOUSING PERSONAL INFORMATION**

13.1 Folders and Records housing Personal Information must not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed, unless the longer retention of the Folder or Record:

- is required or authorised by law;
- is required by Tshiamiso Trust for lawful purposes related to its functions or activities;
- is required by a contract between the parties thereto; or
- is as per consent received from the Data Subject who owns the Personal Information.

13.2 Records housing Personal Information may be retained indefinitely for business, historical, statistical or research purposes provided that Tshiamiso Trust has established appropriate safeguards against the Records being used for any other purposes.

13.3 Each Tshiamiso Trust department or area of operations will be responsible for the correct management of their Folders and Records, including the closing and archiving of these Records when they are no longer needed.

13.4 In order to ensure that the above duties are discharged, all Personnel must ensure that:

- on an ongoing basis they manage the respective life cycles of Folders and Records under their control;
- they establish what record retention periods and related requirements apply to the respective Folders and Records under their control, as per Tshiamiso Trust Records Retention Policy;
- the record retention periods and related requirements are recorded in the department's relevant Department Records Management Register;
- a Folder and Record is formally closed when the matter housed in the Folder or Record comes to an end, which is documented in the relevant Document Management Register;
- a closed Folder or Record is moved to a dedicated archive storage area where the Folder or Record will be retained for the required retention period;
- Folders and Records are only archived in secure storage media;
- only authorized personnel are granted physical and system-based access to archived Folders and Records;
- Folders and Records are archived in areas that are regularly backed up;

- once the prescribed retention period in respect of an archived Folder or Record has expired, the Folder or Record is marked “for deletion or disposal”;
- before a Folder or Record is deleted or destroyed, the department head must obtain permission to delete or destroy said Folder or Record from the Information Officer, which will be reflected in the relevant department Records Management Register;
- each department, once approval for the deletion / destruction of the Folder or Record has been received, via the head of the department, will be responsible for the deletion or destruction of such archived Folder or Record after the expiration of the retention period, unless instructed otherwise by the Information Officer, for example when there is a requirement to place the Folder or Record under a legal or PAIA hold;
- the legal /PAIA hold status must be indicated under the relevant Folder or Record in the relevant Document Management Register;
- during a legal /PAIA hold procedure, the affected Folder or Record must not be destroyed, even if the retention period has expired;
- the deletion / disposal of Folders and Records must ensure the permanent and complete deletion / disposal of all originals and reproductions (including both paper and electronically stored records);
- the department head is responsible for documenting the destruction details under the relevant department Records Management Register.

## **14. OPERATORS**

14.1 Where Tshiamiso Trust makes use of an Operator, in terms of sections 19 to 21 of POPIA, it must ensure that the Operator only uses the Personal Information as per the mandate to Process issued by Tshiamiso Trust, keeps the Personal Information placed under its control, confidential, secure and safe, and that a standard Trust Operator Agreement/Addendum (hereinafter referred to as the "Operator Agreement/Addendum") is concluded between Tshiamiso Trust and the Operator, which sets out the above provisions and any other terms and rules which the Operator will have to follow when Processing Personal Information on behalf of Tshiamiso Trust, which Operator Agreement/Addendum is housed on Tshiamiso Trust website.

14.2 All Personnel must:

- familiarise themselves with the standard Trust Operator Agreement/Addendum;
- ascertain who they use as Operators, now and in the future, include such details under an Operator register, and ensure that all such Operators sign the standard Trust Operator Agreement/Addendum or a similar one which has been approved and signed off by Tshiamiso Trust Legal Department;
- ensure that Operator Agreement/Addendum is followed by an Operator and that where an Operator Agreement/Addendum is breached, bring this to the attention of one's line manager and the Information Officer and following a decision reached by these parties, carry out the planned course of action, which ultimately must aim to protect and secure the Personal Information which is the subject matter of that Operator Agreement/Addendum.

## **15. SHARING PERSONAL INFORMATION WITH THIRD PARTIES**

15.1 Tshiamiso Trust may not share Personal Information with third parties in South Africa, unless:

- there is a legitimate business need to share the Personal Information; or
- the Data Subject has been made aware that his, her or its Personal Information will be shared with others and has, where required, given consent to such sharing; or

- the person receiving the Personal Information has agreed to keep the Personal Information confidential and to use it only for the purpose for which it was shared under the standard Trust Personal Information transfer agreement, which is housed on Tshiamiso Trust website or where acting as an Operator has concluded an Operator Agreement/Addendum with Tshiamiso Trust, before receipt of the Personal Information.

15.2 In order to ensure that the above takes place, Personnel must ensure:

- that where Personal Information is shared externally with a third party, there is a legitimate business need to share the Personal Information; or the Data Subject has been made aware that his, her or its Personal Information will be shared with others and has, where required, given consent to such sharing; or
- or in the absence of the above two situations, has, signed the standard Tshiamiso Trust Personal Information transfer agreement which is concluded with the recipient, before receipt of the Personal Information;
- that where Personal Information is shared with an Operator, that the standard Trust Operator Agreement/Addendum is concluded with the Operator before receipt of the Personal Information;
- that any requested deviations for the standard Tshiamiso Trust Personal Information transfer agreement or the Operator Agreement/Addendum is vetted and approved by Tshiamiso Trust Legal Department;
- when sending emails which contain Personal Information, that they are marked “confidential”, do not contain the Personal Information in the body of the email, whether sent or received, but rather placed in an attachment, which attachment is password protected or encrypted before being transferred electronically;
- that Personal Information is not transferred or sent to any entity not authorised directly to receive it;
- that where Personal Information is to be sent by facsimile transmission, that the recipient has been informed in advance of the transmission and that he or she is waiting by the fax machine to receive the data;
- that where Personal Information is transferred physically, whether in hardcopy form or on removable electronic media, that it is passed directly to the recipient or sent using recorded deliver services and housed in a suitable container marked “confidential”;
- that where Personal Information is shared internally, that adequate measures are put in place to protect the confidentiality and integrity of such information.

## **16. CROSS BORDER TRANSFERS OF PERSONAL INFORMATION**

16.1 Tshiamiso Trust may not transfer Personal Information to another party who is situated outside South Africa, unless

- the Data Subject Consents (under POPIA); or

- the transfer is necessary in order to perform a contract between Tshiamiso Trust and a Data Subject, or for reasons of public interest, or to establish, exercise or defend legal claims or to protect the vital or legitimate interests of the Data Subject in circumstances where the Data Subject is incapable of giving Consent; or
- the country where the Personal Information is being transferred to, provides the Data Subject with the same level of protection as is housed under the data processing laws applicable in South Africa; or alternatively,
- Tshiamiso Trust has concluded a Personal Information data transfer agreement with the recipient of the Personal Information, either in the form of a standard binding corporate rule, or an Operator Agreement/Addendum or a Personal Information transfer agreement, which sets out the rules which apply to the receipt and the subsequent Processing of that Personal Information.

16.2 In order to ensure that the above is followed, Personnel may not transfer Personal Information to areas outside South Africa, unless one of the following controls and safeguards are in place:

- the South African Data Privacy /Personal Information Regulator has issued an “adequacy decision” confirming that the territory or country where Tshiamiso Trust proposes transferring the Personal Information to, has adequate Data Protection laws in place which will afford the Data Subject with the same level of protection as that under POPIA;
- the standard Trust Personal Information data transfer agreement or Operator Agreement/Addendum has been concluded with the recipient of the Personal Information;
- the Data Subject has given Consent (POPIA) to the proposed transfer, having been fully informed of any potential risks;

- the transfer is necessary in order to perform a contract between Tshiamiso Trust and a Data Subject, for reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject in circumstances where the Data Subject is incapable of giving Consent (POPIA).

## **17. REPORTING PERSONAL INFORMATION BREACHES**

- 17.1 In the event of a Personal Information breach, Tshiamiso Trust has a duty to give notice of such breach to the Regulator who is in charge of POPIA, being the Information Regulator (Information Regulator), and to the Data Subject(s) whose Personal Information has been affected as a result of such breach.
- 17.2 Tshiamiso Trust has put in place appropriate procedures to deal with any Personal Information breach and will notify the Information Regulator and/or the Data Subjects, as the case may be, when it is legally required to do so of any breach.
- 17.3 Personnel have a duty to
  - 17.3.1 immediately report through to the Information Officer, any suspected or known Personal Information breach; using the prescribed Tshiamiso Trust data breach report, which report format is annexed hereto marked **Annexure B** and which report must contain the following details:
    - categories and approximate number of Data Subjects concerned;
    - categories and approximate number of Personal Information records concerned;
    - the likely cause of and the consequences of the breach;
    - details of the measures taken, or proposed to be taken, to address the breach including, where appropriate, measures to mitigate its possible adverse effects.
  - 17.3.2 keep such information strictly private and confidential;
  - 17.3.3 ensure that they do not deal with any persons in relation to the Personal Information breach, including any officials or investigators, noting that only the Information Officer with the approval of the CEO or Tshiamiso Trust's Trustees has the right to report any Personal Information or security breach to the Information Regulator and/or the affected Data Subjects, as the case may be and to deal with any person in connection with such matter.

## **18 DATA SUBJECT RIGHTS AND REQUESTS**

18.1 A Data Subject has a number of rights under POPIA in relation to his, her or its Personal Information, including the right to:

- withdraw Consent;
- object to Processing;
- obtain confirmation of Processing and/or access to Personal Information;
- amend, update and delete Personal Information;
- to object to direct marketing;
- be notified of a personal information breach; and
- to complain.

18.2 Tshiamiso Trust has developed, implemented and will maintain certain processes and related forms which give effect to these Data Subject rights, which processes and related forms are contained in the specific and informed Tshiamiso Trust Processing notices which can be found on Tshiamiso Trust website. When a Data Subject is desirous of exercising these rights, then he, she or it must be directed to Tshiamiso Trust website at: <https://www.tshiamisotrust.com/legal/> where the relevant Processing notices and related prescribed forms are housed, which form, once completed must be directed to and handled directly by the Information Officer or his or her deputy, and no other, who will be responsible for dealing with the request and advising the affected Data Subject and/ or any affected Personnel of any decision and outcome in relation to such request.

18.3 Personnel must:

- familiarise themselves with the Data Subjects' rights, and the related processes and forms which need to be followed and completed in order to access these rights;
- take note of and give effect to these processes;
- in particular note that where a Data Subject seeks advices on what Personal Information Tshiamiso Trust holds and which pertains to that Data Subject or where the Data Subject is desirous of accessing this Personal Information, that such right has to be exercised using the "request for access to information" procedure which is described under a law known as the Promotion of Access to Information Act, 2000 (PAIA) and which request procedure is more fully set out under Tshiamiso Trust's PAIA Manual available on Tshiamiso Trust website.



- where asked by any Data Subject to give effect to these rights, do not deal with the request directly but instead direct the Data Subject to the relevant process and form on Tshiamiso Trust website, and provide assistance in so far as completing the form only.

## **19 THE RIGHT TO COMPLAIN**

- 19.1 A Data Subject has to right lodge a complaint with regards to the Processing of his, her or its Personal Information.
- 19.2 Tshiamiso Trust has established for this purpose, an internal compliant resolution procedure.
- 19.3 Should a Data Subject wish to submit a complaint, Personnel must, if contacted by the Data Subject, ask the Data Subject to complete the prescribed “personal information processing complaint” form, which is housed on the Tshiamiso Trust website, and to submit the complaint, once completed, directly to the Information Officer.
- 19.4 On receipt of the complaint, the Information Officer will attempt to hear and resolve the matter, internally and failing resolution will provide the Data Subject with a non-resolution notice.
- 19.5 If the Information Officer and Data Subject are able to resolve the matter, a record setting out the solution will be compiled, and signed by the parties and any other affected persons provided with details of the resolution.
- 19.6 Where the parties are unable to resolve the matter, the Data Subject on receipt of the non-resolution notice, will have the right to refer the complaint to the Information Regulator.

## **20 GOVERNANCE**

- 20.1 Tshiamiso Trust has appointed the below mentioned parties as its Information Officer(s) and Deputy Information Officers, (see Annexure “Information Officers” ) who will be responsible for the following:
  - developing, constructing and once prepared, implementing and overseeing an enterprise-wide Personal Information Processing framework and related roadmap including various Personal Information Processing procedures and policies, including this Policy;
  - monitoring compliance with this Policy, the various Personal Information Processing procedures and the Data Processing law;
  - providing all Personnel with the necessary and required Personal Information Processing training;
  - providing ongoing guidance and advice on Personal Information Processing;

- conducting Personal Information impact assessments when required, including base line risk assessments of all Tshiamiso Trust's Personal Information Processing activities;
- ensuring that all operational and technological Personal Information and data protection standards are in place and are complied with;
- working closely with IT in order to ensure that appropriate technological and operational measures have been implemented in order to ensure the safety and security of all electronically stored Personal Information;
- receiving and considering reports from IT about compliance with all technological and operational data protection standards and protocols;
- be entitled and have authorisation in conjunction with Tshiamiso Trust HR function, to initiate disciplinary proceedings against Personnel who breach any technological and/or organizational and/or operational data protection standard, rule, custom, instruction, policy, practice and/or protocol (verbal, in writing or otherwise), including this Policy;
- review and approve any contracts or agreements which deviate from the standard Tshiamiso Trust Processing documentation;
- attend to requests and queries from Data Subjects, including requests for access to their Personal Information;
- liaising with and/or co-operating with any regulators or investigators or officials who may be investigating a Personal Information or data privacy matter.

20.2 All queries and concerns in relation to the Processing of Personal Information within Tshiamiso Trust operations or concerning Tshiamiso Trust activities, must be taken up with the Information or Deputy Information Officers.

20.3 Tshiamiso Trust's IT department will be responsible for the following:

- conducting cyber security risk assessments including base line risk assessments of all Tshiamiso Trust information technology activities;
- ensuring that adequate and effective IT operational and technological data protection procedures and standards are in place in order to address all IT security risks;
- ensuring that all systems, services and equipment used for Processing and/or storing data adheres to internationally acceptable standards of security and data safeguarding, and is regularly updated to continue to comply with such standards;
- issuing appropriate, clear, and regular rules and directives, whether for Tshiamiso Trust as a whole or a particular part of it, department, person or level of person in relation to any aspect of Tshiamiso Trust work, including password protocols, data access protocols, levels of persons who enjoy access to certain data sign-on procedures, password safeguarding protocols, sign-on and sign-off procedures, log-on and log-off procedures; the description of accessories, applications and equipment that will or may be used, and/or that may not be used under any circumstances, and the like.

- evaluate any third-party services which Tshiamiso Trust is considering or may acquire to Process or store data, e.g., cloud computing services and ensuring that appropriate and effective operational and technological data protection procedures and standards are in place in order to address all IT security risks which may present themselves in respect of these external service providers.

## **21 TRAINING**

21.1 Tshiamiso Trust will conduct regular training sessions covering the contents of the data privacy laws and Tshiamiso Trust related Personal Information Processing policies and procedures, which will be available to all Personnel.

21.2 Personnel must:

- attend the scheduled and offered training;
- do all that is necessary in order to understand the data privacy laws and how they may impact on the Tshiamiso Trust Personal Information Processing activities;
- familiarise themselves with the Tshiamiso Trust Personal Information Processing policies, procedures and prescribed forms;
- ensure that they Process Personal Information in accordance with the Data Processing laws, this Policy, the training, the related policies and procedures and/or any guidelines issued by the Tshiamiso Trust from time to time.

## **22 NON-COMPLIANCE**

- 22.1 Compliance with this Policy and any related procedures and policies is mandatory.
- 22.2 Any transgression of this Policy, and any related procedures and policies, will be investigated and may lead to action being taken against the transgressor.
- 22.3 Further information on the relevant data protection laws, POPIA, Tshiamiso Trust Processing of Personal Information procedures and issues, and Processing Notices, including specific practical guidance on issues of particular relevance to Personnel, can be found on Tshiamiso Trust's website.

## **VERSION AND AMENDMENTS**

This Policy is effective as of 1.....

## **ANNEXURE A**

### **DOCUMENTS AND RECORDS CLASSIFICATION INSTRUCTIONS AND REGISTER FORMATS**

#### **CLASSIFICATION INSTRUCTIONS**

Any person who collects, uses, stores, or transmits Documents and Records has a responsibility to maintain and safeguard such Data.

The first step in establishing the safeguards that are required for a particular type of Documents and Records is to determine the level of sensitivity applicable to such Data. Documents and Records classification is a method of assigning such categories and thereby determining the extent to which the Documents and Records need to be governed, controlled, and secured.

The responsibility for the classification of Documents and Records rests with the Documents and Records owner / business unit where the documents have their origin.

Documents and Records classification, in the context of information security, also addresses the impact to the Trust should such classified Documents and Records be disclosed, altered, or destroyed without authorisation.

The classification of Documents and Records helps determine what baseline security controls are appropriate for safeguarding that Data. All Trust Documents and Records is categorised into one of four sensitivity classifications:

#### **Proprietary Data**

Documents and Records should be classified as Proprietary when this information is restricted to management-approved internal access and protected from external access. Unauthorized access could influence Tshiamiso Trust's operational effectiveness, cause an important financial loss, provide a significant gain to a competitor, or cause a major drop in customer confidence. Information integrity is vital.

Examples of this type of Documents and Records include passwords and information on corporate security procedures; know-how used to process client information; Standard Operating Procedures used in all parts of Tshiamiso Trust's business; all Trust-developed intellectual property, whether used internally or in transactions with third parties.

#### **Confidential Documents and Records**

Documents and Records should be classified as Confidential when the unauthorised disclosure, alteration or destruction of that Documents and Records could cause a significant level of risk to Tshiamiso Trust or its affiliates. Examples of Confidential Documents and Records include Documents and Records protected by state privacy regulations and Documents and Records protected by confidentiality agreements. This also includes

information received from third parties in any form for processing and use . The highest level of security controls should be applied.

Access to Confidential Documents and Records must be controlled from creation to destruction and will be granted only to those identified who require such access to perform their job (“need-to-know”). Access to Confidential Documents and Records must be individually requested and then authorised by the Documents and Records Owner who is responsible for the data.

Confidential Documents and Records is highly sensitive and may have personal privacy considerations or may be restricted by state law. In addition, the negative impact on the institution should this Documents and Records be incorrect, improperly disclosed, or not available when needed is typically very high.

Examples of Confidential/Restricted Documents and Records include salaries and other personnel data; accounting Documents and Records and internal financial reports; confidential customer business Documents and Records and confidential contracts; non- and any information shared in respect thereof; Tshiamiso Trust business plans.

Such Confidential Documents and Records shall also be protected in terms of the Protection of Personal Information Act, 2013, and in accordance with the Trust

POPI Policy.

### **Internal/Private Documents and Records**

This type of Documents and Records can be defined as any information that is proprietary or produced only for use by members of the Trust who have a legitimate purpose to access such data.

Documents and Records should be classified as Internal/Private when the unauthorised disclosure, alteration or destruction of that Documents and Records could result in a moderate level of risk to Tshiamiso Trust or its affiliates. By default, all information assets that are not explicitly classified as Confidential or Public Documents and Records should be treated as Internal/Private Data. A reasonable level of security controls should be applied to Internal Data.

Access to Internal/Private Documents and Records must be requested from, and authorised by, the Documents and Records Owner who is responsible for the data. Access to Internal/Private Documents and Records may be authorised to groups of persons by their job classification or responsibilities (“role-based” access) and may also be limited by one’s department.

Internal/Private Documents and Records is moderately sensitive in nature. Often, Internal/Private Documents and Records is used for making decisions, and therefore it is important this information remain timely and accurate. The risk for negative impact on the Trust should this information not be available when needed is typically moderate. Examples of Internal/Private Documents and Records include official Trust records such as financial reports, human resources information, some research data, unofficial employee records, budget information, internal operating procedures and operational manuals, internal memoranda, emails, reports and other documents, and technical documents such as system configurations and floor plans.

## **Public Documents and Records**

This type of Documents and Records can be defined as any information that may or must be made available to the public, with no legal restrictions on its access or use.

Documents and Records should be classified as Public when the unauthorised disclosure, alteration or destruction of that Documents and Records would result in little or no risk to Tshiamiso Trust and its affiliates. While little or no controls are required to protect the confidentiality of Public Data, some level of control is required to prevent unauthorised modification or destruction of Public Data.

Public Documents and Records is not considered sensitive; therefore, it may be granted to any requester or published with no restrictions. The integrity of Public Documents and Records should be protected. The appropriate Documents and Records Owner must authorise replication or copying of the Documents and Records to ensure it remains accurate over time. The impact on Tshiamiso Trust, should Public Documents and Records not be available is typically low, (inconvenient but not debilitating). Examples of Public Documents and Records include directory information, course information and research publications.

## DATA COLLECTIONS

Data Owners may wish to assign a single classification to a collection of data that is common in purpose or function. When classifying a collection of data, the most restrictive classification of any of the individual data elements should be used. For example, if a data collection consists of an employee's address and ID number, the data collection should be classified as Confidential even though the employee's name and address may be considered Public Data.

## DETERMINING CLASSIFICATION

The goal of information security is to protect the confidentiality, integrity and availability of information assets and systems. Data classification reflects the level of impact to the Trust if confidentiality, integrity or availability of the data is compromised.

POTENTIAL IMPACT	LOW	MODERATE	HIGH
Security Objective			
<b>Confidentiality-</b> Preserving authorised restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	The unauthorised disclosure of information could be expected to have a limited adverse effect on organisational operations, organisational assets or individuals.	The unauthorised disclosure of information could be expected to have a serious adverse effect on organisational operations, organisational assets or individuals.	The unauthorised disclosure of information could be expected to have a severe or catastrophic adverse effect on organisational operations, organisational assets or individuals.



<p><b>Integrity-</b> Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.</p>	<p>The unauthorised modification or destruction of information could be expected to have a limited adverse effect on organisational operations, organisational assets or individuals.</p>	<p>The unauthorised modification or destruction of information could be expected to have a serious adverse effect on organisational operations, organisational assets or individuals.</p>	<p>The unauthorised modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organisational operations, organisational assets or individuals.</p>
<p><b>Availability-</b> Ensuring timely and reliable access to and use of information.</p>	<p>The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organisational operations, organisational assets, or individuals.</p>	<p>The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organisational operations, organisational assets or individuals.</p>	<p>The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organisational operations, organisational assets or individuals.</p>

## INFORMATION HANDLING REQUIREMENTS

The table below defines the required security controls for handling, transmitting, dispatching, protecting, and reproducing classified information assets:

SECURITY CONTROL	INFORMATION CLASSIFICATION			
	Proprietary Data	Confidential	Internal / Private Data	Public data
Access Control	<p>Viewing and modification restricted to authorised individuals as needed for business-related roles.</p> <p>Data Owners or custodian grants permission for access, plus approval from line manager.</p> <p>Authentication and authorization required for access.</p> <p>Confidentiality agreement required.</p>	<p>Viewing and modification restricted to authorised individuals as needed for business-related roles.</p> <p>Data Owners or custodian grants permission for access, plus approval from line manager.</p> <p>Authentication and authorization required for access.</p> <p>Confidentiality agreement required.</p>	<p>Viewing and modification restricted to authorised individuals as needed for business-related roles.</p> <p>Data Owner or custodian grants permission for access, plus approval from the line manager.</p> <p>Authentication and authorization required for access</p>	No restrictions for viewing.
Copying Printing (applies to both paper and electronic)	<p>Data shall only be printed when there is a legitimate need.</p> <p>Copies shall be limited to individuals authorised to access the data and have signed a confidentiality agreement.</p> <p>Information shall not be left unattended on a printer / desk.</p>	<p>Data shall only be printed when there is a legitimate need.</p> <p>Copies shall be limited to individuals authorised to access the data and have signed a confidentiality agreement.</p> <p>Information shall not be left unattended on a printer / desk.</p>	<p>Data shall only be printed when there is a legitimate need.</p> <p>Copies shall be limited to individuals on a need-to-know</p> <p>Information shall not be left unattended on a printer / desk. Control access to print output on copier.</p>	No restrictions

	Control access to print output on copier  Copies shall be labelled as per categorization "Confidential or Proprietary"	Control access to print output on copier.  Copies shall be labelled as per categorization "Confidential or Proprietary"		
Physical Security	<b>Hardcopy:</b> Secure in locked cabinet or location with appropriate physical controls.  Physical access shall be monitored, logged, and to authorised individuals.	<b>Hardcopy:</b> Secure in locked cabinet or location with appropriate physical controls.  Physical access shall be monitored, logged, and to authorised individuals.	<b>Hardcopy:</b> Secure in locked cabinet or location with appropriate physical controls.	System shall be locked or logged out when unattended.
Information storage	Storage on a secure server, cloud <b>recommended</b> . Storage in a secure data Centre or cloud <b>recommended</b> .  Should not store on an individual's workstation, mobile device (cell phones, laptops, iPad, etc.) or removal devices (USB, external hard drives). If stored on a workstation or mobile device, shall use full disk encryption.  Encryption on backup media required. Use restricted access folders,  <b>Mandatory:</b> file password protection for sensitive files at document level	Storage on a secure server or cloud <b>recommended</b> .  Storage in a secure data Centre or cloud <b>recommended</b> .  Should not store on an individual's workstation, mobile device (cell phones, laptops, iPad, etc.) or removal devices (USB, external hard drives) Hardcopy: Secure in locked cabinet or location with appropriate physical controls. Use restricted access folders,  <b>Mandatory:</b> file password protection for	Storage on a secure server or cloud <b>recommended</b> .  Storage in a secure data Centre or cloud <b>recommended</b> . Lock screen when unattended.	Storage in a secure server recommended.  Storage in a secure Data Centre. Lock screen when unattended

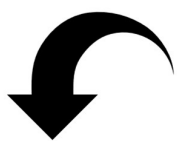
	Hardcopy: Secure in locked cabinet or location with appropriate physical controls.	sensitive files at document level		
--	--	-----------------------------------	--	--

Transmission	Encryption required.  Cannot transmit via email unless encrypted and secure with a digital signature.	Encryption required	Encryption required	No restrictions
Remote access to systems hosting data	Access restricted to local network or VPN  Confidentiality agreement required for remote access by third party for technical reasons.	Access restricted to local network or VPN	Access restricted to local network or VPN	No restrictions

## DOCUMENT RECORDS MANAGEMENT REGISTER FORMAT

<b>Author:</b> Your name	
<b>Title:</b> Name of your project	
<b>Duration:</b> Dates of project	
<b>Classification:</b> See instructions above	
<p><b>1. File Structure</b>  Describe the organization of computer folders for your project.  List the primary folders, and then summarize the organization of their sub-folders.  How will the computer folders for your project be distinguished from other projects and work that you might be involved with?</p> <p><b>Good Practice</b>  Use a system that is logical to you, but simple and self-explanatory to others.  Avoid using the same name for sub-folders as this may lead to the over-writing of their contents.</p>	
<b>2. File Names housed in folder</b>	
<b>Primary Folder name</b>	<b>Location</b>
<b>Sub Folder name</b>	<b>Contents</b>
<b>Sub Folder name</b>	<b>Contents</b>
<b>Sub Folder name</b>	<b>Contents</b>
	<b>Signed:</b> <b>Version:</b>
<b>Date Created:</b>	<b>Date amended:</b>

**The record details must be extracted and inserted in the**  
**DOCUMENT RECORDS MANAGEMENT REGISTER FORMAT**



**DEPARTMENT DETAILS**

**TSHIAMISO TRUST**

**DEPARTMENT NAME**

**AREA WHERE SITUATED**

**HEAD OR MANAGER OF DEPARTMENT**



**POPIA POLICY**

**POLICY NUMBER**

**REVISION NUMBER**

Vol 2

**PAGE NUMBER**

**EFFECTIVE DATE**

40

April 2021

REF. NO	CATEGORY	NAME OF FILE	SPI	PI	STATE AND DATES	FORMAT LOCATION  SERVER / SYSTEM	DETAILS OF PERSONS WHO HAVE ACCESS	ARCHIVE PERIOD	SPECIFIC INSTRUCTION	DESTROYED
<b>CLASSIFICATION</b> <b>See instructions above</b>										
Dept-1	Employees  <b>Folder</b>  Current Employees	Alison Lee / 2016	Yes	Yes	Current  Date  01/02/2019	<b>Hard file</b>  Detail location  <b>Electronic</b>  Detail location		7 years  Indefinite	i.e.  <b>Legal or PAIA Hold</b>  <b>Off Site Storage</b>	<b>Date</b>  <b>Manner</b>  <b>Permission</b>





**POPIA POLICY**

**POLICY NUMBER**

**REVISION NUMBER**

Vol 2

**PAGE NUMBER**

**EFFECTIVE DATE**

41

April 2021

						<b>Copies</b>		Location		
						Detail where located				
						<b>Legal or PAIA hold</b>		n/a		
						<b>Archived</b>		n/a		
						<b>Destroy'</b>	<b>PERSON IN CHARGE</b>		<b>SIGN</b>	



<b>POLICY NUMBER</b>	<b>REVISION NUMBER</b>
	Vol 2
<b>PAGE NUMBER</b>	<b>EFFECTIVE DATE</b>
42	April 2021

**Remark:**

The records maintained by this department were reviewed on .....

All records dated beyond their retention periods have to be destroyed. New record series now being filed have to be added to this schedule and those no longer being filed must have been deleted  
Tshiamiso Trust

**Department:**

**Valid for:**

**Responsible person:**

**Signed off by Information Officer:**



<b>POLICY NUMBER</b>	<b>REVISION NUMBER</b>
	Vol 2
<b>PAGE NUMBER</b>	<b>EFFECTIVE DATE</b>
43	April 2021

## **ANNEXURE B**

### **INCIDENT INVESTIGATION FORM**

This incident report is to be used for all incidents relating to privacy and information security incident management.

Definition of an incident: A threat or event than compromises, damages, or causes a loss of confidential or protected information.

Confidential information: includes proprietary, technical, business, financial, joint-venture, customer and employee information that is not available publicly. It is the employee's responsibility to know what information is confidential and to obtain clarification when in doubt.

Person reporting the incident (can remain anonymous)	
Manager	
Date and time incident occurred	
Date and time incident reported	
Site/ Region	

### **INCIDENT SUMMARY (SHORT STATEMENT OF EVENT)**


### **INCIDENT INVESTIGATION**



<b>POLICY NUMBER</b>	<b>REVISION NUMBER</b>
	Vol 2
<b>PAGE NUMBER</b>	<b>EFFECTIVE DATE</b>
44	April 2021

The following five sections are intended to assist you to clarify the sequence of events immediately preceding the incident. They expand on the details already provided in the summary. Additional pages/ documents can be attached when necessary.

#### **WHO WAS INVOLVED?**


#### **WITNESSES?**


#### **WHAT HAPPENED?**


#### **WHEN DID THE INCIDENT OCCUR?**




<b>POLICY NUMBER</b>	<b>REVISION NUMBER</b>
	Vol 2
<b>PAGE NUMBER</b>	<b>EFFECTIVE DATE</b>
45	April 2021

**WHERE DID THE INCIDENT OCCUR?**


**THE EXISTENCE OR LOCATION OF ANY PROOF THAT MAY EXIST?**


**EXTENT OR CONSEQUENCES OF THE DAMAGE / COMPROMISE ETC**


***Consequences of incidents: Those found in breach of this policy and any associated procedures and guidelines may result in disciplinary actions up to and including dismissal. Legal and criminal actions may also be penalties to individuals who intentionally obtain or disclose protected information without authorization.***

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

**ANNEXURE “INFORMATION AND DEPUTY INFORMATION OFFICERS”**



<b>POLICY NUMBER</b>	<b>REVISION NUMBER</b>
	Vol 2
<b>PAGE NUMBER</b>	<b>EFFECTIVE DATE</b>
46	April 2021

**Name: Kabelo Sedupane**

Postal & Physical address: Block 2, 3 Anerley Road

Parktown, Johannesburg 2193

Telephone number: 010 824 8350

E-mail address: Kabelo.sedupane@tshiamisotrust.com

**Deputy Information Officer Contact Details**


Name: Rhulani Mackaukau

Postal & Physical address: Block 2, 3 Anerley Road

Parktown, Johannesburg 2193

Telephone number: 010 824 8350

E-mail address: Rhulani.mackaukau@tshiamisotrust.com

	<b>POLICY NUMBER</b>	<b>REVISION NUMBER</b>
		Vol 2
	<b>PAGE NUMBER</b>	<b>EFFECTIVE DATE</b>
	47	April 2021



### **POPIA DOCUMENTS IN SUPORT OF THE ABOVE POLICY**

1. POPIA Compliance Framework/Manual
2. Appointment of an Information Officer (IO) and Deputy Information Officer (DIO)
3. Personal Information Impact Assessments and Data Maps where applicable
4. Processing Notices required under section 18
5. Operator Agreement
6. Data Transfer Agreement – cross border
7. Binding Corporate Rules
8. Opt out form
9. Withdrawal of consent
10. Objection notice
11. Complaint form
12. Update to or correction of Personal Information
13. PAIA Manual