POLICY

DESCRIPTION: PROTECTION OF PERSONAL INFORMATION ACT (POPIA)
Revision Version Control

<table>
<thead>
<tr>
<th>Version No.</th>
<th>Last Review Date</th>
<th>Change Request by</th>
<th>Amended by</th>
<th>Change Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>06/02/2014</td>
<td>Management</td>
<td>Jared Appel; Michael Tymvios</td>
<td>Creation</td>
</tr>
<tr>
<td>1.20</td>
<td>23/06/2021</td>
<td>James McAlpine</td>
<td>James McAlpine; Marc Colborne; Jared Appel</td>
<td>New format. Revision version control tables added and completed. Confidentiality level field added. Adapted headings to policy and new contents in sections added based on POPIA. See Table of Contents for section numbers and headings.</td>
</tr>
<tr>
<td>2.00</td>
<td>30/09/2022</td>
<td>James McAlpine</td>
<td>James McAlpine; Marc Colborne; Zanele Khanyile</td>
<td>Removed the POPIA Supplier Agreement and where it’s been referenced have added the DPA. Added Notification of a Security Compromise Form in the Annexures. Language updated to be gender Neutral.</td>
</tr>
<tr>
<td>2.1</td>
<td>24/02/2023</td>
<td>James McAlpine</td>
<td>James McAlpine; Marc Colborne; Zanele Khanyile</td>
<td>Annexure A: Removed Information Officer Appointment Letter; Added Request Form</td>
</tr>
</tbody>
</table>

Approval

<table>
<thead>
<tr>
<th>Approved By</th>
<th>Signature</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>James McAlpine</td>
<td>[Signature]</td>
<td>24/02/2023</td>
</tr>
</tbody>
</table>

© Copyright The Document Warehouse (Pty) Ltd. – All Rights Reserved.
TABLE OF CONTENTS

1. PURPOSE, SCOPE AND USERS

2. REFERENCE DOCUMENTS

3. INTRODUCTION

4. DEFINITIONS

5. GENERAL GUIDING PRINCIPLES

6. RIGHTS OF DATA SUBJECTS

7. INFORMATION OFFICERS

8. SPECIFIC DUTIES AND RESPONSIBILITIES

9. POPIA AUDIT (POPIA RISK ASSESSMENT/ RISK REGISTERS)

10. REQUEST TO ACCESS PERSONAL INFORMATION

11. POPIA COMPLAINTS PROCEDURE

12. DISCIPLINARY ACTION

13. CONTACT PERSON

14. VALIDITY AND DOCUMENT MANAGEMENT

ANNEXURE A: REQUEST FORM

ANNEXURE B: POPIA COMPLAINT FORM

ANNEXURE C: POPIA NOTICE AND CONSENT FORM

ANNEXURE D: EMPLOYEE CONSENT AND CONFIDENTIALITY CLAUSE

ANNEXURE E: SLA CONFIDENTIALITY CLAUSE

ANNEXURE F: INFORMATION OFFICER APPOINTMENT LETTER

ANNEXURE G: NOTIFICATION OF A SECURITY COMPROMISE FORM
1. PURPOSE, SCOPE AND USERS

The users of this document are all employees of The Document Warehouse.

1.1. Purpose

The purpose of this document is to define clear rules with regards to collecting, processing and storing of personal information in accordance with Protection of Personal Information Act 4 of 2013 (“POPIA”).

This policy is to protect The Document Warehouse from compliance risks associated with the protection of personal information, this includes:

- Breaches of confidentiality. i.e., suffering a loss of income where it is found that the personal information of data subjects has been shared or disclosed without the proper authorisation.

- Shortcomings in offering choice. i.e., all data subjects should be free to choose how and for what purpose The Document Warehouse uses information relating to them.

- Damage of reputation. i.e., the organisation could suffer a decline in value following an adverse event, for instance a computer hacker gaining access to personal information held by The Document Warehouse.

This policy demonstrates The Document Warehouse's commitment to protecting the data subject's privacy rights by:

- stating desired behaviour and directing compliance with best practice and the provisions of POPIA.

- creating an organisational culture that recognises privacy as a human right.

- having and continuously assessing internal controls for the purpose of managing the compliance risk in regards to the protection of personal information.

- creating business practices that will provide reasonable assurance that the rights of data subjects are protected and balanced with the legitimate business needs of The Document Warehouse.

- raising awareness via training and providing guidance to individuals who process personal information so that they can act in accordance with POPIA.
assigning specific roles and responsibilities to control owners, including the appointment of an Information Officer and Deputy Information Officers in order to protect the interests of data subjects of The Document Warehouse.

1.2 Scope

This policy applies to:

- The Document Warehouse:
  When referencing The Document Warehouse all entities are included, which are:
  - The Document Warehouse (Pty) Ltd.
  - The Document Warehouse Coastal (Pty) Ltd.
  - The Document Warehouse North West (Pty) Ltd.
  - The Document Warehouse Mpumalanga (Pty) Ltd.
- The Document Warehouse’s POPIA Committee.
- All branches, departments and divisions of The Document Warehouse.
- All contractors, suppliers and other persons acting on behalf of The Document Warehouse.
- The policy’s guiding principles find application in all situations and must be read in conjunction with POPIA as well as the organisation's PAIA manual as required by the Promotion of Access to Information Act (Act No 2 of 2000).
- The legal duty to comply with POPIA's provisions is activated in any situation where there is:
- A processing of personal information entered into a record by or for a responsible person who resides in South Africa.
2. REFERENCE DOCUMENTS

Compliance files, policies and manual are maintained by the compliance function. These include:

- IT Policy.
- Information Security policy.
- PAIA Manual.
- Compliance Manual including all Policies, Processes and Procedures.
- Data Protection Agreement.

Requests for any compliance information or documentation to be submitted to:

The Document Warehouse (Pty) Ltd.

jhb.io@tdw.co.za

The Document Warehouse North West (Pty) Ltd.

pot.io@tdw.co.za

The Document Warehouse Coastal (Pty) Ltd.

cpt.io@tdw.co.za

The Document Warehouse Mpumalanga (Pty) Ltd.

nlp.io@tdw.co.za

3. INTRODUCTION

The right to privacy is an essential human right recognised and protected in South Africa through POPIA.

POPIA aims to promote the protection of privacy through the guiding principles that are intended to be applied to the processing of personal information.

Through the provision of quality goods and services, The Document Warehouse is necessarily involved in the collection, use and disclosure of certain aspects of the personal information of clients, customers, employees and other stakeholders.

A person's right to privacy entails having control over their personal information and being able to conduct their affairs relatively free from undesirable encroachments.
Given the importance of privacy, The Document Warehouse is committed to effectively managing personal information in accordance with POPIA.

4. DEFINITIONS

4.1. Personal Information

Personal information is any information that can be used to reveal a person's identity. Personal information relates to an identifiable, living, natural person, and where applicable, an identifiable, existing juristic person (such as a company), including, but not limited to information concerning:

- race, gender, sex, pregnancy, marital status, national or ethnic origin, colour, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language and birth of a person;
- information relating to the education or the medical, financial, criminal or employment history of the person;
- any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
- the biometric information of the person;
- the personal opinions, views or preferences of the person;
- the views or opinions of another individual about the person;
- correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
- the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.
4.2. Data Subject

This refers to the natural or juristic person to whom personal information relates, such as an employee, individual client, customer or a company that supplies the organisation with products or other goods.

4.3. Responsible Party

The responsible party is the entity that needs the personal information for a particular reason and determines the purpose of and means for processing the personal information. In this case, the organisation is the responsible party.

4.4. Operator

An operator means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party. For example, a third-party service provider that has contracted with the organisation to file documents containing personal information.

4.5. Information Officer

The Information Officer is responsible for ensuring the organisation’s compliance with POPIA. Where no Information Officer is appointed, the head of the organisation will be responsible for performing the Information Officer’s duties. Once appointed, the Information Officer must be registered with the South African Information Regulator established under POPIA prior to performing his or her duties. Deputy Information Officers can also be appointed to assist the Information Officer.

4.6. Deputy Information Officer

The Deputy Information Officer are responsible for assisting the Information Officer ensuring the organisation’s compliance with POPIA. The Information Officer will appoint the Deputy Information Officers and will register them with the information regulator.
4.7. Processing

The act of processing information includes any activity or any set of operations, whether or not by automatic means, concerning personal information and includes:

- the collection, receipt, recording, organisation, 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 any restriction, degradation, erasure or destruction of information.

4.8. Record

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

- Writing on any material;
- Information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored;
- Label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;
- Book, map, plan, graph or drawing;
- Photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced.
4.9. **Filing System**

Means any structured set of personal information, whether centralized, decentralized or dispersed on a functional or geographical basis, which is accessible according to specific criteria.

4.10. **Unique Identifier**

Means any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party.

4.11. **De-Identify**

This means to delete any information that identifies a data subject or which can be used by a reasonably foreseeable method to identify, or when linked to other information, that identifies the data subject.

4.12. **Re-Identify**

In relation to personal information of a data subject, means to resurrect any information that has been de-identified that identifies the data subject, or can be used or manipulated by a reasonably foreseeable method to identify the data subject.

4.13. **Consent**

Means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.

4.14. **Direct Marketing**

Means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of:

- Promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or
• Requesting the data subject to make a donation of any kind for any reason.

4.15. Biometrics
Means a technique of personal identification that is based on physical, physiological or behavioural characterization including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition.

4.16. Child
Means a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him- or herself.

4.17. Competent Person
Means any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child.

5. GENERAL GUIDING PRINCIPLES

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

5.1. Accountability
Failing to comply with POPIA could potentially damage The Document Warehouse's reputation or expose the organisation to a civil claim for damages. The protection of personal information is therefore everybody's responsibility.

The Document Warehouse will ensure that the provisions of POPIA and the guiding principles outlined in this policy are complied with through the encouragement of desired behaviour. However, The Document Warehouse will take appropriate sanctions, which may include disciplinary action, see section 12, against those individuals who through their negligent or intentional
actions and/or omissions fail to comply with the principles and responsibilities stated in this policy.

5.2. Processing limitation

The Document Warehouse will ensure that personal information under its control is processed:

• in a fair, lawful and non-excessive manner, and
• only with the informed consent of the data subject, and
• only for it intended purpose.

The Document Warehouse will inform the data subject of the reasons for collecting their personal information and obtain written consent prior to the processing of personal information. Alternatively, where services or transactions are concluded over the telephone or electronic video feed, The Document Warehouse will state the purpose for which the information will be used, followed by acquiring the data subject's consent.

The Document Warehouse will not share or distribute personal information between separate legal entities, associated organisations or with any individuals that are not involved with facilitating the intended purposes of the information.

Where applicable, the data subject must be informed of the possibility that their personal information will be shared with other aspects of the organisation's business and be provided with the reasons for doing so.

The "POPIA Notice and Consent Form" can be found under Annexure C.

5.3. Purpose specification

All of The Document Warehouse's divisions and operations must be transparent. The Document Warehouse will process personal information only for intended use and legitimate reasons. The Document Warehouse will inform data subjects of the reasons prior to collecting or recording the data subject's personal information.
5.4. Further processing limitation

Personal information will not be processed for a secondary purpose unless it is in line with the original purpose. If the secondary purpose is not in line with the original purpose The Document Warehouse will first obtain additional consent from the data subject to process personal information for the secondary purpose.

5.5. Information quality

The Document Warehouse will take reasonable steps to ensure that all personal information collected is complete, accurate and not misleading. The more important it is that the personal information be accurate, the greater the effort the organisation will put into ensuring accuracy. Where personal information is collected or received from third parties, The Document Warehouse will take reasonable steps to confirm that the information is correct by verifying the accuracy of the information directly with the data subject or by way of independent sources.

5.6. Open communication

The Document Warehouse will take reasonable steps to ensure that data subjects are notified (where applicable) that their personal information is being collected including the purpose for which it is being collected and processed. The Document Warehouse will ensure that it establishes and maintains a "contact us" facility, for instance via its website, for data subjects who want to:

- Enquire whether the organisation holds related personal information, or
- Request access to related personal information, or
- Request the organisation to update or correct related personal information, or
- Make a complaint concerning the processing of personal information.
5.7. Security safeguards

The Document Warehouse will manage the security of its filing system to ensure that personal information is adequately protected. To this end, security controls will be implemented in order to minimize the risk of loss, unauthorized access, disclosure, interference, modification or destruction.

The Document Warehouse will continuously review its security controls which may include testing of protocols and measures put in place to combat cyber-attacks on the organisation’s IT network.

The Document Warehouse will ensure that all paper and electronic records comprising personal information are securely stored and made accessible only to authorized individuals.

All new employees will be required to sign employment contracts containing contractual terms for the use and storage of employee information. Confidentiality agreements will also be included to reduce the risk of unauthorized disclosures of personal information for which the organisation is responsible.

All existing employees will, after the required consultation process has been followed, be required to sign an addendum to their employment contract containing the relevant consent and confidentiality agreements.

Where a supplier who is high risk or deals with our personal information is identified, the identified supplier will need to sign a Data Protection Agreement form either as part of the supplier agreement or on its own.

The Document Warehouse's operators and third-party service providers will be required to enter into service level agreements with the organisation where both parties pledge their mutual commitment to POPIA and the lawful processing of any personal information pursuant to the agreement. An example of “Employee Consent and Confidentiality Clause” for inclusion in The Document Warehouse's employment contracts can be found under Annexure D. An example of an "SLA Confidentiality Clause" for inclusion in The Document Warehouse's service level agreements can be found under Annexure E.
5.8. Data Subject participation
A data subject may request the correction or deletion of his, her or its personal information held by The Document Warehouse. The Document Warehouse will ensure that it provides a facility for data subjects who want to request the correction or deletion of their personal information. Where applicable, the organisation will include a link to unsubscribe from any of its electronic newsletters or related marketing activities. The Document Warehouse can only assist data subjects that we are in direct contact with, where a data subject makes a request and we are not the responsible party of the information we will make the responsible party aware of the request (where reasonably practical).

6. RIGHTS OF DATA SUBJECTS
Where The Document Warehouse is considered the responsible party for a data subjects’ personal information, we will ensure that its clients and customers are made aware of the rights conferred upon them as data subjects. The Document Warehouse will ensure that it gives effect to the following seven rights:

6.1. The right to access Personal Information
The Document Warehouse recognizes that a data subject has the right to establish whether The Document Warehouse holds personal information related to them including the right to request access to that personal information where we are the responsible party. An example of a "Personal Information Request Form" can be found under Annexure A.

6.2. The right to have Personal Information corrected or deleted
The data subject has the right to request, where necessary, that their personal information must be corrected or deleted where The Document Warehouse is no longer authorized to retain the personal information.
6.3. The right to object to the processing of Personal Information

The data subject has the right, on reasonable grounds, to object to the processing of their personal information. In such circumstances, The Document Warehouse will give due consideration to the request and the requirements of POPIA. The Document Warehouse may cease to use or disclose the data subject's personal information and may, subject to any statutory and contractual record keeping requirements, also approve the destruction of the personal information.

6.4. The right to object to Direct Marketing

The data subject has the right to object to the processing of their personal information for purposes of direct marketing by means of unsolicited electronic communications.

6.5. The right to complain to the Information Regulator

The data subject has the right to submit a complaint to the Information Regulator regarding an alleged infringement of any of the rights protected under POPIA and to institute civil proceedings regarding the alleged non-compliance with the protection of his, her or its personal information. An example of a "POPIA Complaint Form" can be found under Annexure B.

6.6. The right to be informed

The data subject has the right to be notified that their personal information is being collected by The Document Warehouse. The data subject also has the right to be notified in any situation where The Document Warehouse has reasonable grounds to believe that the personal information of the data subject has been accessed or acquired by an unauthorized person.
7. INFORMATION OFFICERS

The Document Warehouse will appoint an Information Officer and Deputy Information Officers to assist the Information Officer. The Document Warehouse's Information Officer is responsible for ensuring compliance with POPIA.

There are no legal requirements under POPIA for The Document Warehouse to appoint an Information Officer. Appointing an Information Officer is however, considered to be a good business practice.

Where no Information Officer is appointed, the head of The Document Warehouse (CEO) will assume the role of the Information Officer. Consideration will be given on an annual basis to the re-appointment or replacement of the Information Officer and the re-appointment or replacement of any Deputy Information Officers.

Once appointed, The Document Warehouse will register the Information Officer with the South African Information Regulator established under POPIA prior to performing his or her duties. An example of an "Information Officer Appointment Letter" can be found under Annexure F.

8. SPECIFIC DUTIES AND RESPONSIBILITIES

8.1. POPIA Committee

The Document Warehouse’s POPIA committee cannot delegate its accountability and is ultimately answerable for ensuring that the organisation meets its legal obligations in terms of POPIA. The POPIA committee may however delegate some of its responsibilities in terms of POPIA to management or other capable individuals.

The governing body is responsible for ensuring that:

- The Document Warehouse appoints an Information Officer and relevant Deputy Information Officers.
- All persons responsible for the processing of personal information on behalf of the organisation:
o are appropriately trained and supervised to do so,
   o understand that they are contractually obligated to protect the personal
   information they come into contact with, and
   o are aware that a wilful or negligent breach of this policy’s processes and
   procedures may lead to disciplinary action being taken against them

- Data subjects who want to make enquiries about their personal information
  are made aware of the procedure that needs to be followed should they wish
  to do so.

- The scheduling of a yearly POPIA Audit (POPIA Risk Assessment/Risk
  Registers) in order to accurately assess and review the ways in which The
  Document Warehouse collects, holds, uses, shares, discloses, destroys
  and processes personal information.

8.2. Information Officer

The Document Warehouse's Information Officer is responsible for:

- Taking steps to ensure The Document Warehouse's compliance with the
  provisions of POPIA.

- Keeping the POPIA committee updated about the organisation's
  information protection responsibilities under POPIA. For instance, in the
  case of a security breach, the Information Officer must inform and advise
  the POPIA committee of their obligations pursuant to POPIA.

- Continually analysing privacy regulations and aligning them with the
  organisation's personal information processing procedures. This will
  include reviewing The Document Warehouse's information protection
  procedures and related policies.

- Ensuring that POPIA Audits are scheduled and conducted on a regular
  basis.

- Ensuring that The Document Warehouse makes it convenient for data
  subjects who want to update their personal information or submit POPIA
  related complaints to the organisation. For instance, maintaining a "contact
  us" facility on The Document Warehouse's website.
• Approving any contracts entered into with operators, employees and other third parties which may have an impact on the personal information held by the organisation. This will include overseeing the amendment of The Document Warehouse's employment contracts and other service level agreements. As well as getting suppliers that deal with our personal information to sign the Data Protection Agreement.

• Performing a proper due diligence review prior to contracting with operators or any other third-party service providers to process personal information on the organisation's behalf. For instance, cloud computing services.

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

• Where necessary, working with persons acting on behalf of the organisation to ensure that any outsourced marketing initiatives comply with POPIA.

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

• Organising and overseeing the awareness training of employees and other individuals involved in the processing of personal information on behalf of The Document Warehouse.

• Addressing employees' POPIA related questions.

• Addressing all POPIA related requests and complaints made by The Document Warehouse's data subjects.

• Working with the Information Regulator in relation to any ongoing investigations. The Information Officers will therefore act as the contact point for the Information Regulator authority on issues relating to the processing of personal information and will consult with the Information Regulator where appropriate, with regard to any other matter.

• Addressing any personal information protection queries from journalists or media outlets such as newspapers. The Chief Information Officer must approve all correspondence with journalists or media outlets.
• The Deputy Information Officers will assist the Information Officer in performing their duties.

• Report any security compromises to the information regulator using the form under Annexure H.

8.3. Chief Information Officer

The Document Warehouse's Chief Information Officer is responsible for:

• Ensuring that The Document Warehouse's IT infrastructure, filing systems and any other devices used for processing personal information meet acceptable security standards.

• Ensuring that all electronically held personal information is kept only on designated drives and servers and uploaded only to approved cloud computing services.

• Ensuring that servers containing personal information are sited in a secure location, away from the general office space.

• Ensuring that all electronically stored personal information is backed-up and tested on a regular basis.

• Ensuring that all back-ups containing personal information are protected from unauthorised access, accidental deletion and malicious hacking attempts.

• Ensuring that personal information being transferred electronically is encrypted.

• Ensuring that all servers and computers containing personal information are protected by a firewall and the latest security software.

• Performing regular IT audits to ensure that the security of the organisation's hardware and software systems are functioning properly.

• Performing regular IT audits to verify whether electronically stored personal information has been accessed or acquired by any unauthorised persons.

• Approving and maintaining the protection of personal information statements and disclaimers that are displayed on the organisation's website, including those attached to communications such as emails and electronic newsletters.
8.4. Employees and other persons acting on behalf of The Document Warehouse

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

Employees and other persons acting on behalf of The Document Warehouse are required to treat personal information as a confidential business asset and to respect the privacy of data subjects.

Employees and other persons acting on behalf of The Document Warehouse may not directly or indirectly, utilise, disclose or make public in any manner to any person or third party, either within The Document Warehouse or externally, any personal information, unless such information is already publicly known or the disclosure is necessary in order for the employee or person to perform his or her duties.

Employees and other persons acting on behalf of The Document Warehouse must request assistance from their line manager or the Information Officer if they are unsure about any aspect related to the protection of a data subject’s personal information.

Employees and other persons acting on behalf of The Document Warehouse will only process personal information where:

- The data subject, or a competent person where the data subject is a child, consents to the processing; or
- The processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party; or
- The processing complies with an obligation imposed by law on the responsible party; or
- The processing protects a legitimate interest of the data subject; or
- The processing is necessary for pursuing the legitimate interests of the organisation or of a third party to whom the information is supplied.
Furthermore, personal information will only be processed where the data subject:

- Clearly understands why and for what purpose his, her or its personal information is being collected; and
- Has granted the organisation with explicit written consent to process their personal information.

Employees and other persons acting on behalf of The Document Warehouse will consequently, prior to processing any personal information, obtain a specific and informed expression of will from the data subject, in terms of which permission is given for the processing of personal information.

Informed consent is therefore when the data subject clearly understands for what purpose their personal information is needed and who it will be shared with. Consent can be obtained in written form which includes any appropriate electronic medium that is accurately and readily reducible to printed form.

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

- the personal information has been made public, or
- where valid consent has been given to a third party, or
- the information is necessary for effective law enforcement.

Employees and other persons acting on behalf of The Document Warehouse will under no circumstances:

- Process or have access to personal information where such processing or access is not a requirement to perform their respective work-related tasks or duties.
- Save copies of personal information directly to their own private computers, laptops or other mobile devices like tablets, smart phones, flash disks, external hard drives. All personal information must be accessed and updated from the organisation's central IT infrastructure.
- Share personal information informally. In particular, personal information should never be sent by email, as this form of communication is not secure.
Where access to personal information is required, this may be requested from the relevant line manager or the Information Officer.

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

Employees and other persons acting on behalf of The Document Warehouse are responsible for:

- Keeping all personal information that they come into contact with secure, by taking sensible precautions and following the guidelines outlined within this policy including all applicable information security policies.

- Ensuring that personal information is held in as few places as is necessary. No unnecessary additional records, filing systems and data sets should therefore be created.

- Ensuring that personal information is encrypted prior to sending or sharing the information electronically. The IT Manager will assist employees and where required, other persons acting on behalf of the organisation, with the sending or sharing of personal information to or with authorised external persons.

- Ensuring that all computers, laptops and devices such as tablets, flash drives and smartphones that store personal information are encrypted, password protected and never left unattended. Passwords must be changed regularly and may not be shared with unauthorised persons.

- Ensuring that their computer screens and other devices are switched off or locked when not in use or when away from their desks.

- Ensuring that where personal information is stored on removable storage medias such as external drives, CDs or DVDs that these are kept locked away securely when not being used.

- Ensuring that where personal information is stored on paper, that such hard copy records are kept in a secure place where unauthorised people cannot access it. For instance, in a locked drawer or a filing cabinet.

- Ensuring that where personal information has been printed out, that the paper printouts are not left unattended where unauthorised individuals could see or copy them. For instance, close to the printer.
• Taking reasonable steps to ensure that personal information is kept accurate and up to date. For instance, confirming a data subject's contact details when the client or customer phones or communicates via email. Where a data subject's information is found to be out of date, authorisation must first be obtained from the relevant line manager or the Information Officer to update the information accordingly.

• Taking reasonable steps to ensure that personal information is stored only for as long as it is needed or required in terms of the purpose for which it was originally collected. Where personal information is no longer required, authorisation must first be obtained from the relevant line manager or the Information Officer to delete or dispose of the personal information in the appropriate manner.

• Undergoing POPIA Awareness training from time to time. Where an employee, or a person acting on behalf of The Document Warehouse, becomes aware or suspicious of any security breach such as the unauthorised access, interference, modification, destruction or the unsanctioned disclosure of personal information, they must immediately report this event or suspicion to the Information Officer or one of the Deputy Information Officers, who will in turn report to the Information Officer.

9. POPIA AUDIT (POPIA RISK ASSESSMENT/ RISK REGISTERS)

The Document Warehouse’s Information Officer will schedule periodic POPIA Audits. The purpose of a POPIA audit is to:

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

• Determine the flow of personal information throughout The Document Warehouse. For instance, The Document Warehouse’s various branches, departments, divisions and other associated organisations.

• Redefine the purpose for gathering and processing personal information.

• Ensure that the processing parameters are still adequately limited.
• Ensure that new data subjects are made aware of the processing of their personal information.
• Re-establish the rationale for any further processing where information is received via a third party.
• Verify the quality and security of personal information.
• Monitor the extent of compliance with POPIA and this policy.
• Monitor the effectiveness of internal controls established to manage the organisation's POPIA related compliance risk.

In performing the POPIA Audit, Information Officers will liaise with line managers in order to identify areas within The Document Warehouse's operation that are most vulnerable or susceptible to the unlawful processing of personal information. Information Officers will be permitted direct access to and have demonstrable support from line managers and the organisation's POPIA committee in performing their duties.

10. REQUEST TO ACCESS PERSONAL INFORMATION

Data subjects have the right to:
• Request what personal information the organisation holds about them and why.
• Request access to their personal information.
• Be informed how to keep their personal information up to date.

Access to information requests can be made by email, addressed to the Information Officer. The Information Officer will provide the data subject with a "Personal Information Request Form". Once the completed form has been received, the Information Officer will verify the identity of the data subject prior to handing over any personal information. All requests will be processed and considered against the organisation's PAIA Manual. The Information Officer will process all requests within a reasonable time.
11. POPIA COMPLAINTS PROCEDURE

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

- POPIA complaints must be submitted to the organisation in writing. Where so required, the Information Officer will provide the data subject with a "POPIA Complaint Form".
- Where the complaint has been received by any person other than the Information Officer, that person will ensure that the full details of the complaint reach the Information Officer within one working day.
- The Information Officer will provide the complainant with a written acknowledgement of receipt of the complaint within two working days.
- The Information Officer will carefully consider the complaint and address the complainant's concerns in an amicable manner. In considering the complaint, the Information Officer will endeavour to resolve the complaint in a fair manner and in accordance with the principles outlined in POPIA.
- The Information Officer must also determine whether the complaint relates to an error or breach of confidentiality that has occurred and which may have a wider impact on the organisation's data subjects.
- Where the Information Officer has reason to believe that the personal information of data subjects has been accessed or acquired by an unauthorised person, the Information Officer will consult with the organisation's governing body where after the affected data subjects and the Information Regulator will be informed of this breach.
- The Information Officer will revert to the complainant with a proposed solution with the option of escalating the complaint to the organisation's POPIA committee within seven working days of receipt of the complaint. In all instances, the organisation will provide reasons for any decisions taken and communicate any anticipated deviation from the specified timelines.
• The Information Officer’s response to the data subject may comprise any of the following:
  o A suggested remedy for the complaint,
  o A dismissal of the complaint and the reasons as to why it was dismissed,
  o An apology (if applicable) and any disciplinary action that has been taken against any employees involved.

• Where the data subject is not satisfied with the Information Officer’s suggested remedies, the data subject has the right to complain to the Information Regulator.

• The Information Officer will review the complaints process to assess the effectiveness of the procedure on a periodic basis and to improve the procedure where it is found wanting. The reason for any complaints will also be reviewed to ensure the avoidance of occurrences giving rise to POPIA related complaints.

12. DISCIPLINARY ACTION

Where a POPIA complaint or a POPIA infringement investigation has been finalized, The Document Warehouse may recommend any appropriate administrative, legal and/or disciplinary action to be taken against any employee reasonably suspected of being implicated in any non-compliant activity outlined within this policy.

In the case of ignorance or minor negligence, The Document Warehouse will undertake to provide further awareness training to the employee.

Any gross negligence or the wilful mismanagement of personal information, will be considered a serious form of misconduct for which The Document Warehouse may summarily dismiss the employee. Disciplinary procedures will commence where there is sufficient evidence to support an employee’s gross negligence.

Examples of immediate actions that may be taken subsequent to an investigation include:
  • A recommendation to commence with disciplinary action.
  • A referral to appropriate law enforcement agencies for criminal investigation.
• Recovery of funds and assets in order to limit any prejudice or damages caused.

13. CONTACT PERSON

The following person may be contacted in relation to this policy:
James McAlpine: Group Information Officer
Marc Colborne: Chief Information Officer
jhb.io@tdw.co.za

14. VALIDITY AND DOCUMENT MANAGEMENT

This document is valid as of 22/06/2021
The owner of this document is the Information Officer who must check and, if necessary, update the document at least once a year.
Information Officer
James McAlpine

Signature
ANNEXURE A: REQUEST FORM

Please submit the completed form to the Information Officer:

<table>
<thead>
<tr>
<th>Name:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact Number:</td>
<td></td>
</tr>
<tr>
<td>Email Address:</td>
<td></td>
</tr>
</tbody>
</table>

Please be aware that we may require you to provide proof of identification prior to processing your request. There may also be a reasonable charge for providing copies of the information requested.

A. Particulars of Data Subject

| Name & Surname: |  |
| Identity Number: |  |
| Postal Address: |  |
| Contact Number: |  |
| Email Address: |  |

B. Request

I request the organisation to:

a) Inform me whether it holds any of my personal information
b) Provide me with a record or description of my personal information
c) Correct or update my personal information
d) Destroy or delete a record of my personal information

C. Instructions


D. Signature Page

<table>
<thead>
<tr>
<th>Signature</th>
<th>Date</th>
</tr>
</thead>
</table>

© Copyright The Document Warehouse (Pty) Ltd. – All Rights Reserved.
Policy Number: 00086; Version Number: 2.1; Last Review Date: 24/02/2023;
ANNEXURE B: POPIA COMPLAINT FORM

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

Please submit the completed form to the Information Officer:

<table>
<thead>
<tr>
<th>Name:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact Number:</td>
</tr>
<tr>
<td>Email Address:</td>
</tr>
</tbody>
</table>

Where we are unable to resolve your complaint, to your satisfaction you have the right to direct your complaint to the Information Regulator.
The Information Regulator:
Physical Address:  
Email:  
Website:  

A. Particulars of Complainant

<table>
<thead>
<tr>
<th>Name &amp; Surname:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Number:</td>
</tr>
<tr>
<td>Postal Address:</td>
</tr>
<tr>
<td>Contact Number:</td>
</tr>
<tr>
<td>Email Address:</td>
</tr>
</tbody>
</table>

B. Details of Complaint


C. Desired Outcome


D. Signature Page

<table>
<thead>
<tr>
<th>Signature</th>
<th>Date</th>
</tr>
</thead>
</table>
ANNEXURE C: POPIA NOTICE AND CONSENT FORM

The Document Warehouse understands that your personal information is important to you and that you may be apprehensive about disclosing it. Your privacy is just as important to us and we are committed to safeguarding and processing your information in a lawful manner.

We also want to make sure that you understand how and for what purpose we process your information. If for any reason you think that your information is not processed in a correct manner, or that your information is being used for a purpose other than that for what it was originally intended, you can contact our Information Officer.

You can request access to the information we hold about you at any time and if you think that we have outdated information, please request us to update or correct it.

<table>
<thead>
<tr>
<th>Our Information Officer’s Contact Details:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name:</td>
</tr>
<tr>
<td>Contact Number:</td>
</tr>
<tr>
<td>Email Address:</td>
</tr>
</tbody>
</table>

**Purpose for Processing your Information**

We collect, hold, use and disclose your personal information mainly to provide you with access to the services and products that we provide. We will only process your information for a purpose you would reasonably expect, including:

- To carry out any business functions in regards to our products or services
- Providing you with advice, products and services that suit your needs as requested
- To verify your identity and to conduct credit searches
- To notify you of new products or developments that may be of interest to you
- To confirm, verify and update your details
- To comply with any legal and regulatory requirements

Personal information that is stored with may differ widely however; any information that is provided will only be used for its intended use. For example, if you are purely storing your documents with us, we shall not access the personal information stored unless instructed to do so by you.

**Consent to Disclose and Share your Information**

We may need to share your information to provide advice, reports, analyses, products or services that you have requested. Where we share your information, we will take all precautions to ensure that the third party will treat your information with the same level of protection as required by us.

I hereby authorize and consent to the organisation sharing my personal information with the following persons:

<table>
<thead>
<tr>
<th>D. Signature Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name &amp; Surname</td>
</tr>
</tbody>
</table>

© Copyright The Document Warehouse (Pty) Ltd. – All Rights Reserved. Policy Number: 00086; Version Number: 2.1; Last Review Date: 24/02/2023;
ANNEXURE D: EMPLOYEE CONSENT AND CONFIDENTIALITY CLAUSE

- Personal Information” (PI) shall mean the race, gender, sex, pregnancy, marital status, national or ethnic origin, colour, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language and birth of a person; information relating to the education or the medical, financial, criminal or employment history of the person; any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person; the biometric information of the person; the personal opinions, views or preferences of the person; correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence; the views or opinions of another individual about the person whether the information is recorded electronically or otherwise.

- “POPIA” shall mean the Protection of Personal Information Act 4 of 2013 as amended from time to time.

- The employer undertakes to process the PI of the employee only in accordance with the conditions of lawful processing as set out in terms of POPIA and in terms of the employer's relevant policy available to the employee on request and only to the extent that it is necessary to discharge its obligations and to perform its functions as an employer and within the framework of the employment relationship and as required by South African law.

- The employee acknowledges that the collection of his/her PI is both necessary and requisite as a legal obligation, which falls within the scope of execution of the legal functions and obligations of the employer. The employee therefore irrevocably and unconditionally agrees:
  - That they is notified of the purpose and reason for the collection and processing of his or her PI insofar as it relates to the employer's discharge of its obligations and to perform its functions as an employer.
  - That they consents and authorizes the employer to undertake the collection, processing and further processing of the employee's PI by the employer for the purposes of securing and further facilitating the employee's employment with the employer.
  - The employee consents to the employer's collection and processing of PI pursuant to any of the employer's Internet, Email and Interception policies in place insofar as PI of the employee is contained in relevant electronic communications.
  - To make available to the employer all necessary PI required by the employer for the purpose of securing and further facilitating the employee's employment with the employer.
  - To absolve the employer from any liability in terms of POPIA for failing to obtain the employee's consent or to notify the employee of the reason for the processing of any of the employee's PI.
  - To the disclosure of his/her PI by the employer to any third party, where the employer has a legal or contractual duty to disclose such PI.
  - The employee further agrees to the disclosure of his/her PI for any reason enabling the employer to carry out or to comply with any business obligation the employer may have or to pursue a legitimate interest of the employer in order for the employer to perform its business on a day-to-day basis.
  - The employee authorizes the employer to transfer his/her PI outside of the Republic of South Africa for any legitimate business purpose of the employer within the international community. The employer undertakes not to transfer or disclose his/her PI unless it is required for its legitimate business requirements and shall comply strictly with legislative stipulations in this regard.

- The employee acknowledges that during the course of the performance of his/her services, they may gain access to and become acquainted with the personal information of certain clients, suppliers and other employees. The employee will treat personal information as a confidential business asset and agrees to respect the privacy of clients, suppliers and other employees.

- To the extent that they is exposed to or insofar as PI of other employees or third parties are disclosed to him/her, the employee hereby agree to be bound by appropriate and legally binding confidentiality and non-usage obligations in relation to the PI of third parties or employees.

- Employees may not directly or indirectly, utilize, disclose or make public in any manner to any person or third party, either within the organisation or externally, any personal information, unless such information is already publicly known or the disclosure is necessary in order for the employee or person to perform his or her duties on behalf of the employer.
ANNEXURE E: SLA CONFIDENTIALITY CLAUSE

The Document Warehouse will collect, store and process the personal information of the client for its intended purposes, which includes the use of personal information to carry out our business functions, this is done to provide the best service to you our client and to act in accordance with the “Protection of Personal Information Act 4 of 2013” (POPIA). The client agrees to also use any personal information collected, stored and processed from The Document Warehouse and its stakeholders for its intended purpose in accordance with “POPIA”. The Document Warehouse is willing to share its POPIA policy with the client upon request.
I herewith and with immediate effect appoint you as the Information Officer as required by the Protection of Personal Information Act (Act 4 of 2013). This appointment may at any time be withdrawn or amended in writing.

You are entrusted with the following responsibilities:

- Taking steps to ensure the organisation’s reasonable compliance with the provision of POPIA.
- Keeping the governing body updated about the organisation’s information protection responsibilities under POPIA. For instance, in the case of a security breach, the Information Officer must inform and advise the governing body of their obligations pursuant to POPIA.
- Continually analysing privacy regulations and aligning them with the organisation’s personal information processing procedures. This will include reviewing the organisation’s information protection procedures and related policies.
- Ensuring that POPI Audits are scheduled and conducted on a regular basis.
- Ensuring that the organisation makes it convenient for data subjects who want to update their personal information or submit POPI related complaints to the organisation, to do so. For instance, maintaining a "contact us" facility on the organisation's website.
- Approving any contracts entered into with operators, employees and other third parties which may have an impact on the personal information held by the organisation. This will include overseeing the amendment of the organisation’s employment contracts and other service level agreements.
- Encouraging compliance with the conditions required for the lawful processing of personal information.
- Ensuring that employees and other persons acting on behalf of the organisation are fully aware of the risks associated with the processing of personal information and that they remain informed about the organisation’s security controls.
- Organizing and overseeing the awareness training of employees and other individuals involved in the processing of personal information on behalf of the organisation.
- Addressing employees’ POPIA related questions.
- Addressing all POPIA related requests and complaints made by the organisation’s data subjects.
- Working with the Information Regulator in relation to any ongoing investigations. The Information Officers will therefore act as the contact point for the Information Regulator authority on issues relating to the processing of personal information and will consult with the Information Regulator where appropriate, with regard to any other matter.

I hereby accept the appointment as information officer

<table>
<thead>
<tr>
<th>Name &amp; Surname</th>
<th>Signature</th>
<th>Date</th>
</tr>
</thead>
</table>
ANNEXURE G: NOTIFICATION OF A SECURITY COMPROMISE FORM

FORM SCN1

NOTIFICATION OF A SECURITY COMPROMISE IN TERMS OF SECTION 22 OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013)

Note:

1. Attach documents in support of the notification
2. Complete the form in full as is applicable
3. If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.

<table>
<thead>
<tr>
<th>A</th>
<th>DETAILS OF RESPONSIBLE PARTY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name(s) and Surname/Registered name of responsible party:</td>
<td></td>
</tr>
<tr>
<td>Address:</td>
<td></td>
</tr>
<tr>
<td>Contact Number(s):</td>
<td></td>
</tr>
<tr>
<td>Email Address:</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>B</th>
<th>DETAILS OF INFORMATION OFFICER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full names of information officer</td>
<td></td>
</tr>
<tr>
<td>Registration number of information officer</td>
<td></td>
</tr>
<tr>
<td>Contact Number(s):</td>
<td></td>
</tr>
<tr>
<td>E-mail Address:</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>C</th>
<th>DETAILS OF INFORMATION OFFICER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date of incident</td>
<td></td>
</tr>
<tr>
<td>Date incident reported to Information Regulator</td>
<td></td>
</tr>
<tr>
<td>Explanation for delay in notification to the Regulator, if applicable</td>
<td></td>
</tr>
<tr>
<td>Kindly tick applicable box ✓</td>
<td></td>
</tr>
</tbody>
</table>

© Copyright The Document Warehouse (Pty) Ltd. – All Rights Reserved. Policy Number: 00086; Version Number: 2.1; Last Review Date: 24/02/2023;
<table>
<thead>
<tr>
<th>Type of security compromise</th>
<th>Loss of personal information:</th>
<th>☐</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Damage to personal information:</td>
<td>☐</td>
</tr>
<tr>
<td></td>
<td>Unauthorised destruction of personal information:</td>
<td>☐</td>
</tr>
<tr>
<td></td>
<td>Unlawful access to of personal information:</td>
<td>☐</td>
</tr>
<tr>
<td></td>
<td>Unlawful processing of personal information:</td>
<td>☐</td>
</tr>
<tr>
<td></td>
<td>Other:</td>
<td>☐</td>
</tr>
<tr>
<td></td>
<td>If other, please explain:</td>
<td>____________________________________________</td>
</tr>
<tr>
<td></td>
<td></td>
<td>____________________________________________</td>
</tr>
<tr>
<td></td>
<td></td>
<td>____________________________________________</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description of incident</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Kindly tick applicable box ✓</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type of personal information compromised</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Number of data subjects affected</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

| Method of notification to affected data subjects | Mail to the data subject’s last known physical or postal address; | ☐ |
|                                                   | Sent by e-mail to the data subject’s last known e-mail address; | ☐ |
|                                                   | Placed in a prominent position on the website of the responsible party; | ☐ |
|                                                   | Published in the news media: | ☐ |
## Does the notification provide sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise, including—

<table>
<thead>
<tr>
<th>Description</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>A description of the possible consequences of the security compromise;</td>
<td></td>
</tr>
<tr>
<td>A description of the measures that the responsible party intends to take or has taken to address the security compromise;</td>
<td></td>
</tr>
<tr>
<td>A recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise;</td>
<td></td>
</tr>
<tr>
<td>If known, the identity of the unauthorised person who may have accessed or acquired the personal information;</td>
<td></td>
</tr>
</tbody>
</table>

### Status of compromise:

- Confirmed: ☐  
- Alleged: ☐

## D  
Description of the measures that the responsible party intends to take or has taken to address the security compromise and to protect the personal information of the data subjects from further unauthorised access or use.

## E  
### DECLARATION

I declare that the information contained herein is true, correct and accurate.

SIGNED at ________________ on this the ______ day of ____________________ 20____

________________________     __________________________
Name                                               Designation