



POLICY

– PROTECTION OF PERSONAL INFORMATION (POPIA)

document information

Document approver	:	EXCO
Responsible person	:	Praveen Bajjnath
Document owner	:	Johan Laas
Document number	:	POL_POPIA_001
Version number	:	1.0
Date approved	:	05 April 2021



TABLE OF CONTENTS

- 1. Purpose / Scope.....4
- 2. Policy Statement4
- 3. Related Policies and References5
- 4. Terms and Definitions.....5
- 5. Policy Sections7
 - 5.1. Document User Group7
 - 5.2. Risk.....7
 - 5.3. Policy Application.....7
 - 5.4. Rights of Data Subjects8
 - 5.5. General Guiding Principles9
 - 5.5.1. Accountability.....9
 - 5.5.2. Processing Limitation9
 - 5.5.3. Purpose Specification9
 - 5.5.4. Further Processing Limitation.....10
 - 5.5.5. Information Quality10
 - 5.5.6. Open Communication.....10
 - 5.5.7. Security Safeguards.....10
 - 5.5.8. Data Subject Participation.....11
 - 5.6. Information Officers11
 - 5.7. Specific Duties and Responsibilities11
 - 5.7.1. Governing Body11
 - 5.7.2. Information Officer.....12
 - 5.7.3. IT Operations Manager13
 - 5.7.4. Marketing and Communications Manager.....13
 - 5.7.5. Employees and Persons acting on behalf of Rand Refinery13
 - 5.8. POPIA Audit.....16
 - 5.9. Request to Access Personal Information Procedure.....17
 - 5.10. POPIA Complaints Procedure17
 - 5.11. Disciplinary and Contractual Action.....18
 - 5.12. Legislative Framework.....18
 - 5.13. Annexures.....19
 - 5.13.1. A – Personal Information Request Form.....19
 - 5.13.2. B – POPIA Complaint Form19
 - 5.13.3. C – POPIA Notice and Consent Form.....19
 - 5.13.4. D: Employee Consent and Confidentiality Clause.....19
 - 5.13.5. E: SLA Confidentiality Clause.....21
 - 5.14. Signature and Acknowledgement.....22
- 6. Change Control22



1. PURPOSE / SCOPE

The purpose of this policy is to incorporate the requirements of POPIA into the daily operations of Rand Refinery. This policy is aimed at protecting Rand Refinery from the compliance risks associated with the protection of PI which are listed under the Risk (paragraph 4) section below.

This policy demonstrates Rand refinery's commitment to protecting the privacy rights of Data Subjects in the following manner:

- Through stating desired behaviour and directing compliance with the provisions of POPIA and best practice;
- By cultivating an organisational culture that recognises privacy as a valuable human right;
- By developing and implementing internal controls for the purpose of managing the compliance risk associated with the protection of PI;
- By creating business practices that will provide reasonable assurance that the rights of Data Subjects are protected and balanced with the legitimate business needs of Rand Refinery;
- By assigning specific duties and responsibilities to control owners, including the appointment of an Information Officer and where necessary, Deputy Information Officers, in order to protect the interest of Rand Refinery and Data Subjects; and
- By raising awareness through training and providing guidance to individuals who process PI to that they can act confidently and consistently.

2. POLICY STATEMENT

The Protection of Personal Information Act No. 4 of 2013 ("POPIA") aims to give effect to the constitutional right to privacy by balancing the right to privacy against that of access to information. The right to privacy is an integral human right recognised and protected in the South African Constitution, 1996.

POPIA aims to promote the protection of privacy by providing guiding principles that are intended to be applied to the processing of Personal Information ("PI") in a context-sensitive manner.

Through the provision of quality products and services, Rand Refinery Proprietary Limited ("Rand Refinery") is involved in the collection, use and disclosure of certain aspects of the PI of clients, customers, employees and other stakeholders.

A person's right to privacy entails having control over his or her PI and being able to conduct his or her affairs relatively free from unwanted intrusions.

Given the importance of privacy, Rand Refinery is committed to effectively managing PI in accordance with the provisions of POPIA.



3. RELATED POLICIES AND REFERENCES

For the purpose of this procedure the following references are valid:

- PAIA Policy
- Form_Personal Information Request (Form_POPIA_001)
- Form_POPIA Complaint Form (Form_POPIA_002)
- Form_POPIA Notice and Consent (Form_POPIA_003)

4. TERMS AND DEFINITIONS

For the purpose of this procedure the following terms and definitions apply.

- **Personal Information (PI)**
 - PI is any information that can be used to reveal a person's identity. PI 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;
 - 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;
 - the name of the person if it appears with other PI relating to the person or if the disclosure of the name itself would reveal information about the person
- **Data Subject** – This refers to the natural or juristic person to whom PI relates, such as an individual client, customer or a company that supplies Rand Refinery with material, products or other goods.
- **Responsible Party** – The Responsible Party is the entity that needs the PI for a particular reason and determines the purpose of and means for processing the PI. In this case, Rand Refinery is the Responsible Party.
- **Operator** – An Operator means a person who processes PI 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 Rand Refinery to shred documents containing PI. When dealing with an Operator, it is considered good practice for Rand Refinery, as a Responsible Party, to include an indemnity clause within the contract or mandate.



- **Information Officer –**
 - The Information Officer is responsible for ensuring that Rand Refinery complies with the requirements of POPIA. If an Information Officer is not appointed, the CE of Rand Refinery will be responsible for performing the Information Officer's duties.
 - Upon appointment, the Information Officer must be registered with the South African Information Regulator ("Information Regulator") established under POPIA. Deputy Information Officers can also be appointed to assist the Information Officer.
- **Processing**
 - The act of processing information includes any activity or any set of operations, whether or not by automatic means, concerning PI 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 form;
 - merging, linking, as well as any restriction, degradation, erasure or destruction of information.
- **Record**
 - Means any recorded information, regardless of form or medium, including:
 - Writing on any material;
 - Information produced, recorded or stored by means of any 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 means;
 - Book, map, plan, graph or drawing;
 - Photograph, film, 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.
- **Filing System –** Means any structured set of PI, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria.
- **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.
- **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.
- **Consent –** Means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of PI.
- **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.
- **Biometrics** – Means a technique of personal identification that is based on physical, physiological or behavioural characterisation including fingerprinting, retinal scanning and voice recognition, etc.

5. POLICY SECTIONS

5.1. Document User Group

Rand Refinery Employees, fixed term contractors, visitors, third parties (incl. service providers and suppliers)

5.2. Risk

The following are compliance risks associated with the protection of PI:

- i. Breaches of confidentiality: this is where Rand Refinery could suffer revenue losses where it is found that the PI of Data Subjects has been shared or disclosed inappropriately;
- ii. Failure to offer choice: All Data Subjects should be free to choose how and for what purpose Rand Refinery uses information relating to them;
- iii. Reputational damage: Rand Refinery could suffer a decline in shareholder value following an adverse event such as leaking personal information to an unauthorised person or body held by Rand Refinery.

5.3. Policy Application

This policy and its guiding principles apply to:

- Rand Refinery's governing body (board of directors);
 - All business units, functional areas and departments of Rand Refinery;
 - All employees and contractors;
 - All contractors and suppliers; and
 - All persons acting on behalf of Rand Refinery.
- a) The policy's guiding principles find application in all situations and must be read in conjunction with POPIA as well as Rand Refinery's PAIA Policy as required by the Promotion of Access to Information Act (Act No. 2 of 2000)
 - b) The legal duty to comply with POPIA's provision is activated in any situation where there is processing of PI entered into any record by or for a Responsible Party who is domiciled in South Africa.
 - c) POPIA does not apply in situations where the processing of PI;
 - is concluded in the course of purely personal or household activities, or
 - where the PI has been de-identified.



5.4. Rights of Data Subjects

- a) Where appropriate, Rand Refinery will ensure that its clients or customers are made aware of the rights conferred upon them as Data Subjects in terms of POPIA. Rand Refinery will ensure that it gives effect to the following rights as provided for in terms of POPIA:
- b) The Right to access personal information
 - Rand Refinery recognises that a Data Subject has the right to establish whether Rand Refinery hold PI related to him, her or it, including the right to request access to that PI.
- c) The Right to have PI corrected or deleted
 - The Data Subject has the right to request, where necessary, that his, her or its PI must be corrected or deleted where Rand Refinery is no longer authorised to retain the PI.
- d) The Right to Object to the Processing of PI
 - The Data Subject has the right, on reasonable grounds, to object to the processing of his, her or its PI. In such circumstances, Rand Refinery will give due consideration to the request and the requirements of POPIA. Rand Refinery may cease to use or disclose the Data Subject's PI and may, subject to any statutory and contractual record keeping requirements, also approve the destruction of the PI.
- e) The Right to Object to Direct Marketing
 - The Data Subject has the right to object to the processing of his, her or its PI for the purposes of direct marketing by means of unsolicited electronic communications.
- f) 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 PI.
- g) The Right to be Informed
 - The Data Subject has the right to be notified that his, her or its PI is being collected by Rand Refinery. The Data Subject also has the right to be notified in any situation where Rand Refinery has reasonable ground to believe that the PI of the Data Subject has been accessed or acquired by an unauthorised person.

5.5. General Guiding Principles

All employees and contractors of Rand Refinery and all persons acting on behalf of Rand Refinery as an Operator will at all times be subject to, and act in accordance with, the following guiding principles in terms of POPIA:

5.5.1. Accountability

- a) Failing to comply with the provisions of POPIA could potentially damage Rand Refinery's reputation or expose Rand Refinery to a civil claim for damages. The protection of PI within Rand Refinery is therefore the responsibility of all employees and contractors.
- b) Rand Refinery will ensure that the provisions of POPIA and guiding principles outlined in this policy are complied with through the encouragement of desired behaviour. However, Rand Refinery will take appropriate sanctions which may include disciplinary action, against those



individuals who, through their intentional or negligent actions and/or omissions, fail to comply with the principles and responsibilities outlined in this policy.

- c) Rand Refinery will ensure that the provisions of POPIA and the guiding principles outlined in this policy are complied with through a written contract or mandate with Operators to ensure that Operators are contractually accountable to ensuring compliance with POPIA.

5.5.2. Processing Limitation

- a) Rand Refinery will ensure that PI under its control is processed:
 - in a fair, lawful and non-excessive manner, and
 - only with the informed consent of the Data Subject (to the extent necessary), and
 - only for a specifically defined purpose.
- b) Rand Refinery will inform the Data Subject of the reasons for collecting his, her or its PI and obtain written consent prior to processing the PI (to the extent necessary). Rand Refinery will under no circumstances distribute or share PI between separate legal entities, associated organisations (i.e. subsidiary companies) or with any individuals that are not directly involved with facilitating the purpose for which the PI was originally collected.
- c) Where applicable, the Data Subject must be informed of the possibility that his, her or its PI will be shared with other aspects of Rand Refinery's business and be provided with the reason for doing so.

5.5.3. Purpose Specification

- a) All Rand Refinery's business units and operations must be informed by the principle of transparency.
- b) Rand Refinery will process PI only for specific, explicit defined and legitimate reasons. Rand Refinery will inform Data Subjects of these reasons prior to collecting or recording the Data Subject's PI.

5.5.4. Further Processing Limitation

- a) PI will not be processed for a secondary purpose unless that processing is compatible with the original purpose.
- b) Therefore, where Rand Refinery seeks to process PI it holds for a purpose other than the original purpose for which it was originally collected, and where this secondary purpose is not compatible with the original purpose, Rand Refinery will have to obtain additional consent from the Data Subject in this regard.

5.5.5. Information Quality

- a) Rand Refinery will take reasonable steps to ensure that all PI collected is complete, accurate and not misleading.
- b) The more important it is for the PI to be accurate (e.g. the beneficiary details of a life insurance policy are of the outmost importance), the greater the effort Rand Refinery will put in ensuring its accuracy.



- c) Where PI is collected or received from third parties, Rand Refinery 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.

5.5.6. Open Communication

- a) Rand Refinery will take reasonable steps to ensure that Data Subjects are notified (are at all times aware) that their PI is being collected including the purpose for which it is being collected and processed.
- b) Rand Refinery will ensure that it establishes and maintains a “contact us” facility, for instance via its website or through an electronic helpdesk, for Data Subjects who want to:
 - enquire whether Rand Refinery hold related PI, or
 - request access to related PI, or
 - request Rand Refinery to update or correct related PI, or
 - make a complaint concerning the processing of its PI.

5.5.7. Security Safeguards

- a) Rand Refinery will manage the security of its filing/data record-keeping systems to ensure that PI is adequately protected. To this end, security controls will be implemented in order to minimise the risk of loss, unauthorised access, disclosure, interference, modification or destruction.
- b) Security measures also need to be applied in a context-sensitive manner. For example, the more sensitive the PI, such as medical information or bank account details, the greater the security required.
- c) Rand Refinery will continuously review its security controls, which will include regular testing of protocols and measure put in place to combat cyber-attacks on Rand Refinery’s IT network. Rand Refinery will ensure that all paper and electronic records comprising PI are securely stored and made accessible only to authorised individuals.
- d) All new employees will be required to sign employment contracts containing contractual terms for the use and storage of employee information as PI. Confidentiality clauses will also be included to reduce the risk of unauthorised disclosures of PI for which Rand Refinery is responsible.
- e) All existing employees and contractors will, after the required consultation process has been followed, be required to sign an addendum to their employment agreements/contractor agreements containing the relevant consent and confidentiality clauses.
- f) Rand Refinery’s operators and third-party service providers will be required to enter into service level agreements with Rand Refinery where both parties pledge their mutual commitment to POPIA and lawful processing of any PI pursuant to the agreement.

5.5.8. Data Subject Participation

- a) A Data Subject may request the correction or deletion of his, her or its PI held by Rand Refinery subject to any legal requirements for retention of documents.
- b) Rand Refinery will ensure that it provides a facility for Data Subjects who want to request the correction or deletion of their PI.



5.6. Information Officers

- a) Rand Refinery will appoint an Information Officer and where necessary, one or more Deputy Information Officers to assist the Information Officer.
- b) Rand Refinery's Information Officer is responsible for ensuring compliance with POPIA.
- c) There are no legal requirements under POPIA for an organisation to appoint an Information Officer. Appointing an Information Officer is however, considered to be a good business practice, particularly within larger organisations.
- d) Where an Information Officer is not appointed, the CE of Rand Refinery by default will assume the role of the Information Officer.
- e) Once appointed, Rand Refinery will register the Information Officer with the Information Regulator established under POPIA prior to performing his or her duties.

5.7. Specific Duties and Responsibilities

5.7.1. Governing Body

- a) Rand Refinery's governing body cannot delegate its accountability and is answerable for ensuring that Rand Refinery meets its legal obligation in terms of POPIA.
- b) The governing body may however delegate some of its responsibility in terms of POPIA to management or other capable individuals. The governing body is responsible for ensuring that:
 - Rand Refinery appoints an Information Officer, and where necessary, a Deputy Information Officer;
 - All persons responsible for the processing of PI on behalf of Rand Refinery;
 - Are appropriately trained and supervised to do so;
 - Understand that they are contractually obligated to protect PI they come into contact with, and
 - Are aware that 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 PI are made aware of the procedure that needs to be followed should they wish to do so, and
 - Periodic POPIA audits are scheduled in order to accurately assess and review the ways in which Rand Refinery collects, holds, uses, shares, discloses, destroys and processes PI.

5.7.2. Information Officer

Rand Refinery's Information Officer is responsible for:

- i. Taking steps to ensure Rand Refinery's reasonable compliance with the provision of POPIA;
- ii. Keeping the governing body updated about Rand Refinery'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 its obligations pursuant to POPIA;
- iii. Continually analysing privacy regulations and aligning them with the Rand Refinery's PI processing procedures. This will include reviewing Rand Refinery's protection procedure and related policies;



- iv. Ensuing that POPIA audits are scheduled and conducted on a regular basis;
- v. Ensuring that Rand Refinery makes it convenient for Data Subjects who want to update their PI or submit POPIA related complaints to Rand Refinery. For instance, maintaining a “contact us” facility on Rand Refinery’s website;
- vi. Noting any contracts entered into with Operators, employees and other third parties which may have an impact on the PI held by Rand Refinery. This will include overseeing the amendment of Rand Refinery’s employment/contractor contracts and other service level agreements;
- vii. Encouraging compliance with the conditions required for the lawful processing of PI;
- viii. Ensuring that employees and other persons acting on behalf of Rand Refinery are fully aware of the risks associated with the processing of PI and that they remain informed about Rand Refinery’s security controls;
- ix. Organising and overseeing the awareness training of employees and other individuals involved in the processing of PI related questions;
- x. Addressing all POPIA related enquiries;
- xi. Addressing all POPIA related requests/complaints made by Rand Refinery’s Data Subjects; and
- xii. Working with the Information Regulator in relation to any ongoing investigations. The Information Officer will therefore act as the contact point for the Information Regulator authority on issues relating to the processing of PI and will consult with the Information Regulator where appropriate, with regard to any other matter. The Deputy Information Officer(s) will assist the Information Officer in performing his or her duties.

5.7.3. IT Operations Manager

For purposes of complying with the provisions of POPIA and the guiding principles outlined in this policy, Rand Refinery’s IT Operations Manager is responsible for:

- i. Ensuring that Rand Refinery’s IT General Governance and Control are adhered to, user permissions, network and end point devices access and security used for processing PI meet acceptable security standards and with controlled access;
- ii. Ensuring that all electronically held PI is kept only on designated drives and servers and uploaded only to approved cloud computing services;
- iii. Ensuring that servers containing PI are situated in a secure location, away from the general office space;
- iv. Ensuring that all electronically stored PI is backed-up and tested on a regular basis;
- v. Ensuring that all back-ups containing PI are protected from unauthorised access, accidental deletion and malicious hacking attempts;
- vi. Ensuring that PI being transferred electronically is encrypted;
- vii. Ensuring that all servers and computers containing PI are protected by a firewall and satisfactory security software;
- viii. Performing regular IT audits to ensure that the security of Rand Refinery’s hardware and software systems are functioning properly;
- ix. Performing regular IT audits to verify whether electronically stored PI has been accessed or acquired by any unauthorised persons; and



- x. Performing a proper due diligence review prior to contracting with Operators or any other third-party service providers to process PI on Rand Refinery behalf, for example, cloud computing services.

5.7.4. Marketing and Communications Manager

For purposes of complying with the provisions of POPIA and the guiding principles outlined in this policy, Rand Refinery's Marketing and Communications Manager is responsible for:

- i. Approving and maintaining the protection of PI statements and disclaimers that are displayed on Rand Refinery's website, including those attached to communications such as emails and electronic newsletters;
- ii. Addressing any PI protection queries from journalists or media outlets such as newspapers;
- iii. Where necessary working with persons acting on behalf of Rand Refinery to ensure that any outsourced marketing initiatives comply with POPIA.

5.7.5. Employees and Persons acting on behalf of Rand Refinery

- a) Employees and persons acting on behalf of Rand Refinery may, during the course of the performance of their services to Rand Refinery, gain access to and become acquainted with the PI of certain clients, suppliers and other employees.
- b) Employees and persons acting on behalf of Rand Refinery are required to treat PI as a confidential business asset and to respect the privacy of Data Subjects.
- c) Employees and persons acting on behalf of Rand Refinery may not directly or indirectly, utilise, disclose or make public in any manner to any persons or third party, either within Rand Refinery or externally, any PI, unless such information is already publicly known or disclosure is necessary in order for the employee or person to perform his or her duties.
- d) Employees and persons acting on behalf of Rand Refinery must request assistance from their line manager, POPIA Champion or Information Officer if they are unsure about any aspect related to the protection of a Data Subject's PI.
- e) POPIA Champions are appointed by EXCO and are amongst others, responsible for preparing information in respect of the status of POPIA compliance, monitoring POPIA risk mitigation progress and organising POPIA compliance related events or training within their individual departments or business units.
- f) Employees and persons acting on behalf of Rand Refinery may only process PI 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 interest of Rand Refinery or of a third party to whom the information is supplied.
- g) Furthermore, PI may only be processed where the Data Subject:
 - Clearly understands why and for what purpose his, her or its PI is being collected; and



- Has granted Rand Refinery with explicit written or verbally recorded consent to process his, her or its PI.
- h) Employees and persons acting on behalf of Rand Refinery will consequently, prior to processing any PI, obtain specific and informed expression of will from the Data Subject to the extent necessary in terms of which permission is given for the processing of PI.
- i) Informed consent is therefore given when the Data Subject clearly understands for what purpose his, her or its PI is needed and who it will be shared with.
- j) Consent can be obtained in written form, which includes any appropriate electronic medium that is accurately and readily reducible to printed form.
- k) Consent to process a Data Subject's PI must be obtained directly from the Data Subject, except where:
- The PI has been made public, or
 - Where valid consent has been given to a third party, or
 - Pursuing the legitimate interest of Rand Refinery, or
 - The information is necessary for effective law enforcement.
- l) Employees and persons acting on behalf of Rand Refinery will under no circumstance:
- Process or have access to PI where such processing or access is not a requirement to perform their respective work-related tasks or duties;
 - Save copies of PI directly to their own private computers, laptops or other mobile devices like tablets or smart phones. All PI must be accessed and updated from Rand Refinery's central database of a dedicated server;
 - Share PI informally. In particular, PI should never be sent by email, as this form of communication is not secure. Where access to PI is required, this may be requested from the relevant line manager, POPIA Champion or the Information Officer.
 - Transfer PI outside of South Africa without express permission from the Information Officer. Employees and persons acting on behalf of Rand Refinery are responsible for:
 - Keeping all PI that they come into contact with secure, by taking sensible precautions and following the guidelines outlined in this policy;
 - Ensuring that PI is held in a few places as is necessary. No unnecessary additional records, filing systems and data sets should therefore be created;
 - Ensuring that PI is encrypted prior to sending or sharing the information electronically. The IT Operations Manager will assist employees and where required, persons acting on behalf of Rand Refinery, with the sending or sharing of PI to or with authorised external persons;
 - Ensuring that all computers, laptops and devices such as tablets, flash drives and smartphones that contains PI are 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 PI is stored on removable storage medias e.g. external drives/CD's/DVDs, that these are kept locked away securely when not in use;
 - Ensuring that where PI is stored on paper, that such hard copy records are kept in a secure place where unauthorised people cannot access it, for example, in a locked drawer of a filing cabinet;



- Ensuring that where PI has been printed out, that the paper printouts are not left unattended where unauthorised individuals could read or copy them;
 - Taking reasonable steps to ensure the PI is kept accurate and up to date. For instance, confirming a Data Subject's contact details when the client or customer phone or communicates via email. Where a Data Subject's information is found to be out of date, authorisation must be first obtained from the relevant line manager, POPIA Champion or the Information Officer to update the information accordingly;
 - Taking reasonable steps to ensure that PI is stored only for as long as it is needed or required in terms of relevant legislation and/or the purpose for which it was originally collected. Where PI is no longer required, authorisation must first be obtained from the relevant line manager or the Information Officer to delete or dispose of the PI in the appropriate manner;
 - Undergoing POPIA awareness training from time to time.
- m) Where an employee, or a person acting on behalf of Rand Refinery, becomes aware or suspicious of any security breach such as the unauthorised access, interference, modification, destruction or the unsanctioned disclosure of PI, he or she must immediately report such event or suspicion to the Information Officer or the Deputy Information Officer.

5.8. POPIA Audit

- a) Rand Refinery's Information Officer will schedule periodic POPIA audits.
- b) The purpose of a POPIA audit is to:
- i. Identify the processes used to collect, record, store, disseminate and destroy PI;
 - ii. Determine the flow of PI throughout Rand Refinery, for example, Rand Refinery's various departments, functional areas;
 - iii. Redefine the purpose for gathering and processing PI;
 - iv. Ensure that the processing parameters are still adequately limited;
 - v. Ensure that new Data Subjects are made aware of the processing of their PI;
 - vi. Re-establish the rationale for any further processing where information is received via a third party;
 - vii. Verify the quality and security of PI;
 - viii. Monitor the extent of compliance with POPIA and this policy (including any changes to POPIA or applicable laws within South Africa);
 - ix. Monitor the effectiveness of internal controls established to manage Rand Refinery's POPIA related compliance risk.
- c) In performing the POPIA audit, the Information Officer will liaise with line managers in order to identify areas within in Rand Refinery's operation that are most vulnerable or susceptible to the unlawful processing of PI.
- d) The Information Officer and Deputy Information Officer(s) will be permitted direct access to and have demonstrable support from line managers and Rand Refinery's governing body in performing their duties.



5.9. Request to Access Personal Information Procedure

- a) Data Subjects have the right to:
 - i. Request what PI Rand Refinery holds about them and why;
 - ii. Request access to their PI, and
 - iii. Be informed how to keep their PI up to date.
- b) Access to information requests can be made by email, addressed to the Information Officer via the website of Rand refinery. The Data Subject must complete and submit the “Personal Information Request Form” Annexure A (attached hereto) for processing such PI.
- c) Once the completed form has been received, the Information Officer will verify the identity of the Data Subject prior to handling over any PI. All requests will be processed and considered against Rand Refinery’s PAIA Policy.
- d) The Information Officers will process all requests within a reasonable time subject to the circumstances of the request in question.

5.10. POPIA Complaints Procedure

Data Subjects have the right to complain in instances where any of their rights under POPIA have been infringed upon. Rand Refinery takes all complaints in this regard very seriously and will address all POPIA related complaints in accordance with the following procedure:

- i. POPIA complaints must be submitted to Rand Refinery in writing. Where so required, the Information Officer will provide the Data Subject with a “POPIA Complaint Form” Annexure B (attached hereto).
- ii. Where the complaint has been received by any person other than the Information Officer, that person will ensure that that the complaint reach the Information Officer within 1 working day;
- iii. The Information Officer will carefully consider the complaint and address the complainant’s concerns. 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 and this policy;
- iv. 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 Rand Refinery’s and/or Rand Refinery’s Data Subjects;
- v. Where the Information Officer has reason to believe that the PI of a Data Subject has been accessed or acquired by an unauthorised person, the Information Officer will consult with Rand Refinery’s governing body without delay, whereafter the affected Data Subjects and the Information Regulator will be informed of this breach in writing without delay;
- vi. The Information Officer will revert to the complainant with a proposed solution with the option of escalating the complaint to Rand Refinery’s governing body within 7 working days of receipt of the complaint. In all instances, Rand Refinery will provide reasons for any decisions taken and communicate any anticipated deviation for the specified timelines;
- vii. The Information Officer’s response to the Data Subject may comprise any of the following:
 - A suggested remedy for the complaint;
 - A dismissal of the complaint and the reasons as to why it was dismissed;



- An apology (if applicable) and any disciplinary/contractual action that has been taken against employees or contractors 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 that the avoidance of occurrences giving rise to POPAI related complaints.

5.11. Disciplinary and Contractual Action

- a) Where a POPIA complaint or a POPIA infringement investigation has been finalised, Rand Refinery may recommend any appropriate administrative, contractual, legal/or disciplinary action to be taken against any employee or contractor reasonably suspected of being implicated in any non-compliant activity outlined within this policy.
- b) In the case of ignorance or minor negligence, Rand Refinery will undertake to provide further awareness training to the employee or contractor concerned.
- c) Any gross negligence or the wilful mismanagement of PI, will be considered a serious form of misconduct for which Rand Refinery may summarily suspend the employee or terminate the contractors' services. Disciplinary procedures (in respect of employees) or contractual termination procedures (in respect of contractors) will commence where there is enough evidence to support an employee's or contractor's gross negligence or wilful mismanagement of PI.
- d) Examples of immediate actions that may be taken after an investigation include:
 - A recommendation to commence disciplinary action contract termination (as the case may be);
 - A referral to appropriate law enforcement agencies for criminal investigation;
 - Recovery of funds and assets in order to limit any prejudice or damages caused.

5.12. Legislative Framework

Rand Refinery manages its legislative framework within its defined regulatory and legislative framework as defined within its Compliance Risk Management Framework.



5.13. Annexures

5.13.1. A – Personal Information Request Form

Please refer to Form_Personal Information Request (Form_POPIA_001) available on The Document Desk

5.13.2. B – POPIA Complaint Form

Please refer to Form_POPIA Complaint Form (Form_POPIA_002) available on The Document Desk

5.13.3. C – POPIA Notice and Consent Form

Please refer to Form_POPIA Notice and Consent Form (Form_POPIA_003) available on The Document Desk

5.13.4. D: Employee Consent and Confidentiality Clause

- "Personal Information" (PI) shall mean the race, gender, sex, pregnancy, marital status, national or ethnic origin, color, 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 he/she 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 he/she consents and authorizes the employer to undertake the collection, processing and further processing of employee's PI by the employer for the purposes of securing and further facilitating the employee's employment with the employer.
- Without derogating from the generality of the foretasted, 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, he/she 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 he/she 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 organization 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.

5.13.5. E: SLA Confidentiality Clause

- "Personal Information" (PI) shall mean the race, gender, sex, pregnancy, marital status, national or ethnic origin, color, 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 parties acknowledge that for the purposes of this agreement that the parties may come into contact with, or have access to PI and other information that may be classified, or deemed as private or confidential and for which the other party is responsible. Such PI may also be deemed or considered as private and confidential as it relates to any third party who may be directly or indirectly associated with this agreement. Further, it is acknowledged and agreed by the parties that they have the necessary consent to share or disclose the PI and that the information may have value.
- The parties agree that they will at all times comply with POPIA's Regulations and Codes of Conduct and that it shall only collect, use and process PI it comes into contact with pursuant to this agreement in a lawful manner, and only to the extent required to execute the services, or to provide the goods and to perform their respective obligations in terms of this agreement.
- The parties agree that it shall put in place, and at all times maintain, appropriate physical, technological and contractual security measures to ensure the protection and confidentiality of PI that it, or its employees, its contractors or other authorized individuals comes into contact with pursuant to this agreement.
- Unless so required by law, the parties agree that it shall not disclose any PI as defined in POPIA to any third party without the prior written consent of the other party, and notwithstanding anything to the contrary contained herein, shall any party in no manner whatsoever transfer any PI out of the Republic of South Africa.



5.14. Signature and Acknowledgement

By signing this document, I acknowledge that I have read and understood the above terms of this policy.

SIGNED AT:	
DATE:	
NAME AND SURNAME:	
SIGNATURE:	

6. CHANGE CONTROL

UPDATED	DATE UPDATED	KEY CHANGES MADE	VERSION N°
Thembelihle Matsoso	2021/03/05	New Policy	

[End of document]