POLICY

PROTECTION OF PERSONAL INFORMATION

DOCUMENT REF: DWR-P-31

TABLE OF CONTENTS

PROTECTION OF PERSONAL INFORMATION POLICY

1. DEFINITIONS

1.1 DATA SUBJECT refers to the personal information of a person.

1.2 POPIA refers to the Protection of Personal Information Act 4 of 2013.

1.3 PROCESSING means any activity, whether automatic or manual, concerning personal information, such as:

a) the collection, receipt, recording, organization, collation, storage, updating or modification, retrieval, alteration, consultation, or use.

b) Distribution or making available in any other form; or

c) merging, linking, as well as restriction, degradation, erasure, or destruction of information.

1.4 RECORD means any recorded information-

a) irrespective of manual or electronic, including any of the following.

(i) writing of any material.

(ii) information produced, recorded, or stored by means of:

- any tape-recorder
- computer equipment,
- any other material derived from information produced, recorded, or stored.

(iii) labels, markings or any other form of identification

(iv) books, maps, plans, graphs, or drawings.

(v) photographs, films, tapes or other visual devices

b) in the possession or under the control of a responsible person irrespective of who created it.

1.5 RESPONSIBLE PERSON means any person who determines the purpose and means for processing personal information.

1.6 PERSONAL INFORMATION means any information applicable to a person, including, but not limited to:

a) Personal – name, race, gender, sex, pregnancy, marital status, national, ethnic, social origin, colour, sexual orientation, age, physical or mental health, wellbeing, disability, religion,

conscience, belief, culture, language, date of birth, identification number, gender symbol, e-mail address, physical address, telephone number, location information, online identifier, and the biometric information.

b) Education and employment - medical, financial, criminal and employment history

c) Personal opinions – personal views, preferences, confidential correspondence and the views or opinions of other individuals.

1.7 INFORMATION OFFICER means the person who is responsible for ensuring that Dwarsrivier Chrome Mine is compliant with POPI Act.

1.7.1 The appointed, Information Officer must register with the South African Information regulator prior performing his or her duties.

1.7.2 A Deputy information Officer should be appointed to assist the Information Officer.

2. PURPOSE

2.1 The main purpose of this policy is to provide guidance to employees with regards to requirements and guidelines of processing and storing of a data subject's personal information.

2.2 Management will ensure that each employee carries out their duties in accordance with the guidelines of POPIA.

2.3 POPIA will regulate the functionalities of the right to privacy and access to information.

2.4 This policy will assist employees to understand the conditions that must be adhered to when processing and storing personal information.

2.5 This policy will assist employees to remedy errors that were made when processing personal information

3. SCOPE AND OBJECTIVE OF THE POLICY

3.1 This policy is applicable to all employees of Dwarsrivier Chrome Mine, including:

- temporary employees
- contractors
- service providers
- and any persons acting on behalf of Dwarsrivier Chrome Mine.

3.2 The above mentioned are required to familiarize themselves with the policy's requirements and undertake to comply with POPIA.

4. RIGHTS OF DATA SUBJECTS

4.1 A Data subject has the right to have his / her personal information processed in accordance with POPIA including the right to:

a) Be notified when personal information is collected, accessed or requested by an unauthorized person.

b) Request access to his / her personal information from the responsible person.

c) Request, to amend, or delete his / her personal information.

d) Object, on “reasonable grounds” the processing of his / her personal information.

e) Object to the redirecting of their personal information to be used for:

- Purposes of direct marketing; or
- Direct marketing by means of unsolicited electronic communications.

f) Not be subjected to a decision made based on the automated processing of his or her personal information.

g) Submit a complaint to the relevant responsible person regarding the suspected interference with the personal information.

4.2 Should an employee of Dwarsrivier Chrome Mine request access to their personal information such request should be made on the relevant form.

5. CONDITIONS FOR LAWFUL PROCESSING OF PERSONAL INFORMATION

All employees and persons acting on behalf of Dwarsrivier Chrome Mine will always be subject to, and act in accordance with, the following guiding principles:

5.1 ACCOUNTABLITY

5.1.1 Dwarsrivier Chrome Mine’s employees are to ensure that personal information is processed in accordance with POPI Act.

5.1.2 Dwarsrivier Chrome Mine must audit the processes used to collect, record, store, publish and destroy personal information.

5.1.3 Dwarsrivier Chrome Mine must ensure the integrity and safekeeping of personal information that is in its possession.

5.1.4 Dwarsrivier Chrome Mine must ensure that a data subject’s information is kept safe, undamaged and not unlawfully accessed.

5.1.5 All Dwarsrivier Chrome Mine employees responsible for personal information must adhere to processing conditions of POPIA.

5.2 PROCESSING LIMITATION

5.2.1 Lawfulness of processing:

Personal information must be processed lawfully and in a reasonable manner that does not infringe the privacy of the data subject.

a) Processing is deemed lawful if used for the intended purpose.
b) Information to be processed must be adequate, relevant and not excessive.
c) Personal Information may only be processed for any of the following grounds:
(i) The Data Subject consents to processing.
(ii) Conclusion of a contract.
(iii) Complies with the legal responsibility of Dwarsrivier Chrome Mine.
(iv) Protects a legitimate interest of the Data Subject.
(v) Data subject consent is not required if it relates to legal processes or if the information is contained in a public record.

5.2.2 Special Personal Information includes:

a) Religious,
b) Values,
c) Political beliefs.
d) Race or ethnic origin.
e) Trade union membership.
f) Health
g) Sex life
h) Biometric information (including but not limited to blood type, fingerprints, DNA, retinal scanning, voice recognitions, photographs).
i) Criminal behavior.
j) Information concerning a minor.

5.2.3 Dwarsrivier Chrome Mine may only process Special Personal Information under the following circumstances:

a) The Data Subject has consented to processing.
b) The Special Personal Information was made public by the Data Subject.
c) Necessary for legal processes
d) Historical, statistical or research reasons
e) If the processing of race or ethnic origin, is to comply with legislation.

5.2.4 All Data Subjects have the right to:

a) refuse or withdraw their consent to the processing of their Personal Information.

b) object at any time to the processing of their Personal Information, unless required by legislation.

5.2.5 Should the Data Subject withdraw consent, Dwarsrivier Chrome Mine shall immediately refrain from processing the Personal Information.

5.3 PURPOSE SPECIFICATION

5.3.1 Personal Information must be collected for a specific purpose intended for.

5.3.2 Data Subjects must be made aware of the purpose for which the information will be used for.

5.3.3 The purposes for collecting Data Subjects Personal Information can be for the following:

a) Administration of agreements.

b) Providing products and services.

c) FICA legislation

d) Satisfaction research

e) Legal proceedings

f) Staff administration

g) Keeping of accounts and records

5.3.4 Retention and Restriction of Records:

a) Record of Personal Information must be kept according to the set time frame.

b) Once the retention period has lapsed, Dwarsrivier Chrome Mine must destroy or delete a record of personal information.

c) Dwarsrivier Chrome Mine must ensure that the destruction or deletion of Personal Information must be done according to the set standard.

5.4 FURTHER PROCESSING LIMITATION

5.4.1 Further processing of Personal Information must be according to the initial purpose for which it was collected.

5.4.2 To assess if further processing is in line with the initial purpose of collection, Dwarsrivier Chrome Mine must consider the following:

a) The intended further processing and the initial purpose for which the information has been collected must be aligned.

b) The nature of the information concerned.

c) The consequences of the intended further processing for the data subject.

d) How the information was collected; and

e) Any contractual rights and obligations between the parties.

5.4.3 Further processing of Personal Information is not aligned with the purpose of collection if:

a) The information is resulting from a public record or has been made public by the data subject.

5.4.4 Further processing is necessary in the following instances:

a) To avoid biasness to comply to legislation.

b) To comply with legal obligations imposed by law.

c) To comply with court proceedings.

d) To comply with Protection Services proceedings.

5.5 INFORMATION QUALITY

5.5.1 Personal Information obtained from Data Subjects must be complete, accurate, not misleading, and up to date.

5.5.2 Employees should ensure the following when submitting and collecting Personal Information:

a) Personal Information is dated when received.

b) Acknowledge receipt of information.

c) Changes to information records should be dated.

d) Irrelevant or unwanted Personal Information should be deleted or destroyed.

5.5.3 Personal Information should be stored securely, either on a secure electronic database or in a secure physical filing system or both.

5.6 OPENNESS

5.6.1 Documentation

a) Responsible persons must ensure documentation under their control is up to date and kept for the duration as stipulated.

b) Responsible persons must ensure that the Data Subjects are aware of:

(i) The reason for which information is being collected .

(ii) The source from which the information is collected.

(iii) The contact details of Dwarsrivier Chrome Mine site where the data is kept.

(iv) Whether or not the supply of the information by data subject is voluntary or mandatory.

(v) The consequences of failure to provide the information.

(vi) Any law authorizing or requiring the collection of the information.

(vii) The intention of Dwarsrivier Chrome Mine to share the information to a third party and the level of protection.

(viii) The Data Subject has the right to access or rectify the information collected.

(ix) The Data Subject has the right to object (with reasonable justification) to the processing of their Personal Information

(x) Should the Data Subject be unhappy with the way their Personal Information is processed or stored, they have the right to lodge a complaint to the responsible person.

5.7 SECURITY SAFEGUARDS

5.7.1 The responsible person must ensure the integrity and confidentiality of all Personal Information in his/ her possession, by:

a) Identifying reasonable risks to information and report to Protection Services.

b) Implementing control measures for protecting sensitive personal information.

5.7.2 Written records:

a) Personal Information records should be kept in access-controlled areas.

b) When in use, Personal Information records should not be left unattended “Clean Desk Policy”

c) Personal Information which is no longer required should be shredded.

d) Any loss, theft or unauthorized access to Personal Information must be reported immediately to the responsible person.

5.7.3 Electronic Records:

a) Personal Information must be saved on a secure electronic drive.

b) Personal Information should not be saved on individual computers, laptops, or hand-held devices.

c) All computers, laptops and hand-held devices should be access protected.

5.7.4 Loss or theft of computers,

a) Any loss or theft of computers, laptops or other devices which may contain Personal Information must be immediately reported to Protection Services.

b) Protection Services will notify the IT Department

c) IT Department will then remotely delete the information.

5.7.5 IT Department will continuously review its security controls.

5.7.6 Security controls will include regular testing of protocols and measures to combat cyberattacks on the IT network.

5.7.7 Dwarsrivier Chrome Mine's IT department is responsible for:

a) Ensuring that the IT infrastructure, electronic filing system and any other devise used for processing personal information meet acceptable security standards.

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

c) Ensuring that all servers containing personal information are stored in a secure location, away from the general office space.

d) Ensuring that all back-ups containing personal information are protected from unauthorized access and malicious hacking attempts.

e) Ensuring that personal information being transmitted electronically is encrypted.

f) Performing regular IT audits to ensure that the security of the firm's hardware and software systems are functioning.

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

5.8 DATA SUBJECT PARTICIPATION

5.8.1 Data Subjects have the right to request an opportunity to amend or delete their Personal Information as per Annexure "A".

5.8.2 All requests for amendments must be submitted to the responsible person. Dwarsrivier Chrome Mine shall disclose the requested Personal Information. The responsible person must ensure that the update of the personal information.

a) On receipt of adequate proof.

b) Within a reasonable time.

6. GENERAL DESCRIPTION OF INFORMATIONS SECURITY MEASURES

6.1 The IT Department must ensure that the Dwarsrivier Chrome Mine employees use up to date technology to protect the confidentiality, integrity and availability of the Personal Information of all employees. These measures include:

a) Firewalls.

b) Virus protection software and updated protocols.

c) Encryption on data at rest and in transit.

d) Logical and physical access control.

e) Secure setup of hardware and software making up the IT infrastructure.

f) Outsourced Service Providers who process Personal Information on behalf of Dwarsrivier Chrome Mine are contracted to implement security controls.

7. ACCESS TO PERSONAL INFORMATION

7.1 All individuals and entities may request access, amendment or deletion of their own Personal Information. Any requests should be directed, to the Responsible Person.

7.2 A Responsible Person may refuse the request to Personal Information on the following grounds:

7.2.1 Protecting Personal Information that the Mine holds about a third party, including a deceased person.

7.2.2 Protecting commercial information.

7.2.3 If disclosure of a record:

(i) Would endanger the life or safety of a person.

(ii) Would influence belief or harm the security, property, or transport.

(iii) Would impact on the protection of the public safety.

(iv) If controlled in legal proceedings

(v) Would harm the commercial or financial interest of the Mine.

(vi) Would put the Mine at a disadvantage in contracts or negotiations.

(vii) Is a computer programme, and

(viii) If it contains information about research being carried out on behalf of a third party or Dwarsrivier Chrome Mine.

7.3 Records that cannot be found or do not exist:

7.3.1 Should a Data Subject request the Mine to search for a record and it is believed that the record does not exist or cannot be found, the requestor must be notified.

8. IMPLEMENTATION GUIDELINES:

8.1 Training and dissemination of information

a) All employees will be trained in POPIA during induction for new employees and during refresher training every 18 months.

b) Modifications and updates to data protection and information sharing policies, legislation or guidelines will be done as and when available.

8.2 Employee contracts

8.2.1 All new employees will sign a confidentiality undertaking with regards to the use of personal information.

9. INFORMATION OFFICER:

9.1 Dwarsrivier Chrome Mine appointed a Deputy Information Officer and where necessary, a Delegate/ Representative will assist the Deputy the Information Officer.

9.2 The Deputy Information Officer is responsible for ensuring compliance with POPI Act.

9.3 The Deputy Information Officer or his/ her delegate/ representative is to attend to any complaints issued to him / her.

10. DESTRUCTION OF DOCUMENTS:

10.1 Documents may be destroyed according to the retention period specified in "Annexure A"

10.2 Each department is responsible for disposing of its documents and electronic records, which must be done on a regular basis. Files must be checked prior to disposing, original documents must be returned to the employee unless there is a valid reason.

10.3 The unused documents must be shredded.

10.4 Deletion of electronic records must be done in consultation with the IT Department.

11. DISCIPLINARY ACTION:

11.1 Where a POPI Act complaint or investigation has been finalized, Protection Services may recommend appropriate action such as legal and / or disciplinary action to be taken against any employee suspected of being implicated in any non-compliant activity outlined within the policy.

11.2 In the case of ignorance or minor negligence, the Responsible Person will undertake to provide further awareness training to address such issues.

11.3 Any gross negligence or the willful mismanagement of personal information will be handled according to the company's Disciplinary Procedure.

Human Resources Manager	Date: 29/05/2023	**General Manager**	Date: 30/05/2023

Annexure "A"

12. STATUTORY RETENTION PERIODS

Legislation	Document Type	Period
Companies Act	• Any documents, accounts, books, writing, records, or other information that a company is required to keep in terms of the Act. • Notice and minutes of all shareholders meeting, including resolutions adopted and documents should be made available to shareholders. • Copies of reports presented at the annual general meeting of the company. • Copies of annual financial statements required by the Act. • Copies of accounting records as required by the Act. • Record of directors and past directors, after the director has retired from the company. • Written communication to shareholders. • Minutes and resolutions of directors' meetings, audit committee and directors' committees. • Registration certificate. • Memorandum of Incorporation and alterations and amendments. • Rules. • Registers and uncertified registers. • Register of company secretary and auditors and • Regulated Companies (companies to which chapter 5, part B, C and Takeover Regulations apply) – Register of disclosure of person who holds beneficial interest equal to or more than 5% that class issued.	6 Years Indefinitely
Consumer Protection Act	• Full names, physical address, postal address, and contact details. • ID number and registration number.	3 Years

	• Contact details of public officer in case of a juristic person. • Service rendered. • Cost to be recovered from the consumer. • Frequency of accounting to the consumer. • Amounts, sums, values, charges, fees, remuneration specified in monetary terms. • Conducting a promotional competition as per Section 36(11)(b) and Regulation 11 of Promotional Competitions	
Financial Intelligence Centre Act	• Whenever a reportable transaction is concluded with a customer, the institution must keep record of the identity of the customer. • If the customer is acting on behalf of another person, the identity of the person on whose behalf the customer is acting and the customer's authority to act on behalf of that other person, record must be kept of such transaction. • If another person is acting on behalf of the customer, the identity of that person and that other person's authority to act on behalf of the customer, record must be kept for such transaction. • The way the identity of the persons referred to above was established, The nature of that business relationship or transaction must be recorded. • In the case of a transaction, the amount involved and the parties to that transaction must be recorded. • All accounts that are involved in the transactions concluded by that accountable institution during that business relationship and that single transaction must be recorded. • The name of the person who obtained the identity of the person transacting on behalf of the accountable institution must be recorded. • Any document or copy of a document obtained by the accountable institution must be recorded.	5 Years

Compensation for Occupational Injuries and Diseases Act	• Register, record or reproduction of the earnings, time worked, payment for fixed term work and overtime and other prescribed particulars of all the employees. • Section 20(2) documents that: -Health and safety committee recommendations made to an employer in terms of issues affecting the health of employees and of any report made to an inspector in terms of the recommendation; -Records of incidents reported at work	4 Years 3 Years
Basic Conditions of Employment Act	• Section 29(4): -Written particulars of an employee after termination of employment must be kept. • Section 31: • -Employee's name and occupation; • -Time worked by each employee; • -Remuneration paid to each employee; • -Date of birth of any employee under the age of 18 years.	3 Years
Employment Equity Act	• Records in respect of the company's workforce, employment equity plan and other records relevant to compliance with the Act. • Section 21 report which is sent to the Director General.	3 Years
Labour Relations Act	• Records to be retained by the employer are the collective agreements and arbitration awards. • An employer must retain prescribed details of any strike, lock-out or protest action involving its employees. • Any records of disciplinary transgressions of each employee specifying the nature of the actions taken by the employee and the reasons for the actions must be retained	3 Years Indefinite
Unemployment Insurance Act	• Employers must retain personal records of current employees in terms of their names, identification number, monthly remuneration and address where the employee is employed.	5 Years
Tax Administration Act	• Section 29 of the Act documents that: - The responsible person need to observe the requirements of the Act, that are specifically required under a Tax Act by	5 Years

	the Commissioner and which are made in the public notice. -Are. -Such action, will enable SARS to be satisfied that the person has observed the requirements	
Income Tax Act	• Amount of remuneration paid or due by him to the employee. • The amount of employee's tax deducted or withheld from the remuneration paid or due. • The income tax reference number of that employee. • Any further prescribed information. • Employer Reconciliation return.	5 Years
Value Added Tax Act	• Where a vendor's basis of accounting is changed, the vendor shall prepare lists of debtors and creditors showing the amounts owing to the creditors at the end of the tax period immediately preceding the changeover period. • Importation of goods, bill of entry, other documents prescribed by the Custom and Excise Act and proof that the VAT charge has been paid to SARS must be recorded. • Vendors are obliged to retain records of all goods and services, rate of tax applicable to the supply, list of suppliers or agents, invoices and tax invoices, credit and debit notes, bank statements, deposit slips, stock lists and paid cheques. • Documentary proof substantiating the zero rating of supplies must be recorded. • Where a tax invoice, credit, or debit note, has been issued in relation to a supply by an agent or a bill of entry as described in the Customs and Excise Act, the agent shall maintain sufficient records to enable the name, address and VAT registration number of the principal to be ascertained.	5 Years

DOCUMENT CONTROL

Originator:	Cilliers le Roux
Approved by:	Esther Sibuyi
Date requested:	2023/05/24

CHANGE CONTROL

Change Request Number	DETAILS OF CHANGES MADE TO POLICY
	New Policy.

DOCUMENT APPROVAL

Human Resource Manager: 

General Manager: 

Date: 30/05/2023