

PROTECTION OF PERSONAL INFORMATION ACT (POPI ACT) POLICY

INDEX

1. DEFINITIONS
2. INTRODUCTION
3. APPLICABILITY
4. INFORMATION OFFICER
5. INFORMATION OFFICER RESPONSIBILITIES
6. UNDERSTANDING WHAT IS MEANT BY THE TERM "PERSONAL INFORMATION"
7. PROCESSING OF PERSONAL INFORMATION
8. PROCESSING LIMITATIONS
9. DE-IDENTIFYING PERSONAL INFORMATION
10. THE DATA SUBJECT'S RIGHT TO ACCESS TO PERSONAL INFORMATION
11. FORBIDDEN USES OF DATA SUBJECT'S PERSONAL INFORMATION
12. COMPANY'S RIGHT TO ACCESS INFORMATION
13. BREACH OF SECURITY/ UNAUTHORISED ACCESS TO INFORMATION
14. CORPORATE POLICY GUIDELINE
 - 14.1. ACCEPTABLE USES OF PERSONAL INFORMATION
 - 14.2. UNACCEPTABLE USES OF PERSONAL INFORMATION
 - 14.3. QUERIES AND CLARIFICATION OF POLICY
15. POSSIBLE OFFENCES

Link to the POPI ACT: <https://popia.co.za/>



1. DEFINITIONS

In this Policy, unless the context indicates a contrary intention, the following words and expressions bear the meanings assigned to them and cognate expressions bear corresponding meanings –

- 1.1. **"Act"** means the Protection of Personal Information Act, Act No. 4 of 2013 (as amended);
- 1.2. **"Company"** means SIMROX Steel and Pipe, EBM Steel and Manufacturing, Simrox Property Holdings and Esheshayo Trading, all considered as a private company duly registered and incorporated in the Republic of South Africa;
- 1.3. **"data subject"** means the person to whom personal information relates;
- 1.4. **"Directors"** means directors of the Company appointed to the Board;
- 1.5. **"Employee/s/ Contractor/s"** means any person, including a contractor, who works for the Company and who receives, or is entitled to receive, any remuneration; and any other person who in any manner assists in carrying on or conducting the business of the Company;
- 1.6. **"Information Officer"** means the designated compliance officer appointed by the Company to address compliance with the Act, from time to time;
- 1.7. **"this Policy"** means this Protection of Personal Information ("POPI") policy and any addendum thereto as may be amended by the Company and signed by the parties from time to time;
- 1.8. **"Responsible Party/Employee"** means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.

2. INTRODUCTION

This policy describes the Company's guidelines with regard to:-

- 2.1. Use personal information in the office;
- 2.2. Access to and disclosure of personal information sent or received by employees or contractors of the Company with use of the Company email system;
- 2.3. The processing of personal information; and
- 2.4. How to protect the Company from the risks of breach of security and/or unauthorised access to personal information.

3. APPLICABILITY

This policy applies to all Employees and/or Contractors of the Company.

4. INFORMATION OFFICER

- 4.1. The Company duly appoints Q Pelser as its Information Officer.
- 4.2. All Employees and/or Contractors may refer any queries, concerns or information of potential or actual breaches of personal information to the Information Officer.

5. INFORMATION OFFICER RESPONSIBILITIES

- 5.1. To encouragement compliance, by the Company and employees alike, with the conditions for the lawful processing of personal information;
- 5.2. To handle requests made to the Company pursuant to this Act;
- 5.3. To work with the Regulator (established in terms of the Act) in relation to investigations conducted pursuant to Chapter 6 of the Act in relation to the Company; and
- 5.4. To ensure compliance by the Company with the provisions of POPI; and as may be prescribed.

6. UNDERSTANDING WHAT IS MEANT BY THE TERM “PERSONAL INFORMATION”

6.1. Personal information refers to a wide array of data belonging to a natural or juristic person, including but not limited to:

- 6.1.1. Identity and/or passport number;
- 6.1.2. Date of birth and age;
- 6.1.3. Phone number/s (including cellular phone number);
- 6.1.4. Email address/es;
- 6.1.5. Physical address;
- 6.1.6. Postal address;
- 6.1.7. Age, Gender, Race and Ethnicity;
- 6.1.8. Photos, voice recordings, video footage (also CCTV), biometric data;
- 6.1.9. Marital/Relationship status and Family relations;
- 6.1.10. Criminal record;
- 6.1.11. Private correspondence;
- 6.1.12. Religious or philosophical beliefs including personal and political opinions;
- 6.1.13. Employment history and salary information;
- 6.1.14. Financial information;
- 6.1.15. Education information;
- 6.1.16. Medical history including, blood type, and
- 6.1.17. Membership to organisations/unions.

6.2. The scope of the Act seems narrowed by the definition of personal information, but this is not the truth. One must remember that the types of personal information listed by the Act as set out in the list above is not a closed list of personal information to which the Act will apply. Information not listed above may still be deemed personal information.

7. PROCESSING OF PERSONAL INFORMATION

7.1. The Company is fully compliant with the Act and has invested a lot of resources to ensure that the Employees and/or Contractors understand how to handle a client's personal information. All Employees and/or Contractors must follow the following guidelines when dealing with data subject's personal information:

- 7.1.1. The personal information requested must only be used for lawful purposes;
- 7.1.2. The personal information must be processed for a purpose which is adequate, relevant and not excessive;
- 7.1.3. The personal information may only be collected with the data subject's consent. The burden of proof rests with the Employees and/or Contractors, to prove that the information was obtained with the data subject's consent.
- 7.1.4. The Company and Employees and/or Contractors may only collect personal information that is necessary for a specific purpose;
- 7.1.5. Personal information must not be retained longer than necessary, except if it is required by law or is for a lawful purpose related to the Company's functions or activities or it is agreed upon in terms of contractual agreement; and
- 7.1.6. The personal information in the Company's records should be updated as and when the data subject provides new or updated personal information.

8. PROCESSING LIMITATIONS

8.1. No Employees and/or Contractors may use the data subject's personal information in any way that may be seen as revealing special information deemed to be insulting, disruptive, or offensive by other persons, or harmful to morale.

8.2. The scope of processing special personal information is further limited by the Act and thereby the Company forbidding any of the following actions:

- 8.2.1. Collection of personal information of minors;
- 8.2.2. Collection of personal information regarding the data subject's religious or philosophical beliefs;
- 8.2.3. Collection of personal information identifying the data subject's trade union membership or political opinions;
- 8.2.4. Collection of personal information related to the data subject's sexual life, health, or biometric details;
- 8.2.5. Collection of personal information revealing race or ethnic origin;
- 8.2.6. Collection of personal information revealing criminal record behaviour.

8.3. Unless processing is carried out with the consent of the data subject referred to in clause 8.2:

- 8.3.1. processing must be necessary for the establishment, exercise or defence of a right or obligation in law;
- 8.3.2. processing must be necessary to comply with an obligation of international public law;
- 8.3.3. processing must be for historical, statistical or research purposes to the extent that:

- 8.3.3.1. the purpose serves a public interest and the processing is necessary for the purpose concerned;
- 8.3.3.2. it appears to be impossible or would involve a disproportionate effort to ask for consent, and sufficient guarantees are provided for to ensure that the processing does not adversely affect the individual privacy of the data subject to a disproportionate extent;

- 8.3.4. the information must have deliberately been made public by the data subject; or
- 8.3.5. prior authorisation must have been given.

9. DE-IDENTIFYING PERSONAL INFORMATION

- 9.1. The Company has a responsibility to ensure that information that is outdated or no longer needed, is discarded in manner that will no longer identify the data subject. The process will be called de-identifying information.
- 9.2. De-identifying means to delete any information that identifies the data subject's personal information which can be used or manipulated by a reasonably foreseeable method to identify the data subject or can be linked by a reasonably foreseeable method to other information that identifies the data subject.
- 9.3. Archived information records are stored securely on or offsite and a certificate of destruction will be obtained for each archived file/ batch of personal information destroyed.
- 9.4. It is imperative that each and every Employee and/or Contractor takes all the necessary precautions to ensure the above-mentioned protocols are adhered to. Should the Company receive any complaints of failure to protect the data subject's information, the claim must be disproved before the Information Officer. The consequence thereof is that the Employees and/or Contractors tasked with handling the specific information will be found guilty of contravening this policy, the penalty thereof could lead to a written warning.

9.5. The Company's complaints policy that should be followed in the event of a complaint is as follows:

- 9.5.1. The complaint must be reported to the Information Officer immediately;
- 9.5.2. The Information Officer must report the complaint to the Director(s);
- 9.5.3. The Employees and/or Contractors implicated must furnish the Information Officer with written representations of the Employees and/or Contractors statement under oath;
- 9.5.4. The Information Officer will liaise with the Regulator for any further developments regarding the matter.

10. THE DATA SUBJECT'S RIGHT TO ACCESS TO PERSONAL INFORMATION

- 10.1. The owner of personal information can request that the Company provide them with the record, or a description of the personal information, the identity of any third party who may have access or had access to their personal information.
- 10.2. The Company has created a request form which must be completed by the data subject requesting the above-mentioned access to information. The request form is marked annexe B.

11. FORBIDDEN USES OF DATA SUBJECT'S PERSONAL INFORMATION

- 11.1. The Employee or Contractor may not use the Company's access to any data subject's personal information for personal gain on any such purposes as soliciting or proselytising for commercial ventures, religious or personal causes or outside organisations or other similar, non-job-related solicitations. If the Company discovers that any Employee or Contractor misusing the information available in the Company's systems, that Employee and/or Contractor will be subject to disciplinary action, which may include dismissal.
- 11.2. Should an Employee or Contractor be suspected of contravening this policy, the Company may at its sole discretion access any device which the Employee or Contractor uses to conduct business to investigate the matter further.

12. COMPANY'S RIGHT TO ACCESS INFORMATION

1. The Company respects the individual privacy of its Employees and/or Contractors. However, Employee and/or Contractor privacy does not extend to the Employee's and/or Contractor's work-related conduct or to the use of Company provided equipment or supplies.
2. The electronic mail system has been installed by the Company to facilitate business communications. Although each Employee and/or Contractor has an individual password to access this system, it belongs to the Company and the contents of e-mail communications are accessible at all times by the Company management for any business purpose. These systems may be subject to periodic unannounced inspections and should be treated like other shared filing systems. All system passwords and encryption keys must be available to the Company management and the designated IT personnel, and the Employee and/or Contractor may not use passwords that are unknown to their supervisor or the designated IT personnel or install encryption programs without turning over encryption keys to their supervisor your designated IT personnel. All e-mail messages are Company records. The contents of e-mail, properly obtained for legitimate business purposes, may be disclosed within the Company without the Employee's and/or Contractor's permission.
3. Therefore, the Employee and/or Contractor should not assume that messages or telephone calls are confidential. Back-up copies of e-mail may be maintained and referenced for business and legal reasons.

13. BREACH OF SECURITY / UNAUTHORISED ACCESS TO INFORMATION

- 13.1. Should the Company experience any security breach, it is required, by law, to notify the Regulator; and the data subject(s) whose information have been affected by the breach, unless the identity of such data subject(s) cannot be established.
- 13.2. Therefore, the Employee and/or Contractor should report any known or suspected breach of information to the appointed Information Officer.
- 13.3. Failure to report the aforementioned breach will subject the Employee and/or Contractor in transgression to disciplinary action, which may include dismissal.
- 13.4. The Company has established a complaints process to deal with allegations of leaked information. This will be addressed by the Compliance Officer.

14. CORPORATE POLICY GUIDELINE

14.1. ACCEPTABLE USES OF PERSONAL INFORMATION

14.1.1. The Company provides access to its server and e-mail access is intended to be for business reasons only. The Company encourages the use of the server and e-mail because they make communication more efficient and effective. However, the server and e-mail are Company property, and their purpose is to facilitate Company business. Every Employee and/or Contractor has a responsibility to maintain and enhance the Company's public image and to use Company e-mail and access to the server in a productive manner. To ensure that all Employees and/or Contractors are responsible, the following guidelines have been established for using e-mail and the server. Any improper use of the server or e-mail is not acceptable and will not be permitted.

14.1.2. The Employee and/or Contractor acknowledges that:-

14.1.2.1. The Company may be held vicariously liable for the acts of its Employees and/or Contractors, even where the Company is not at fault, for any damages caused by the Employee's and/or Contractor's conduct;

14.1.2.2. Employees and/or Contractors may not make representations to third parties or the public beyond the scope of their normal responsibilities or actual authority;

14.1.2.3. Methods other than email must be used to communicate special personal information.

14.2. UNACCEPTABLE USES OF PERSONAL INFORMATION

14.2.1. The Company acknowledges that Employees and/or Contractors need reasonable access to data subjects' personal information in order to conduct their tasks.

14.2.2. The Employees and/or Contractors may not process the Employee's and/or Contractor's personal information without obtaining the requisite consent, following the protocols discussed in this policy and in the Act.

14.3. QUERIES AND CLARIFICATION OF POLICY

14.3.1. Where an employee is uncertain as to the content of this policy or requests further clarification of issues which are addressed in this policy they are required to contact the Compliance Officer for clarification.



15. POSSIBLE OFFENCES

- 15.1. The Employee and/or Contractor must note that should they fail to adhere to this policy, they may be disciplined and/or dismissed or deleted from the Company's data base and may face action bought by the Information Regulator which mat see them liable to face a fine or imprisonment.



Appendix: Protection of Personal Information Act Policy – To be Signed and returned to the Information Officer of the Company

I have received a copy of Company's Protection of Personal Information Act Policy on the _____ of _____ 20____.

I recognise and understand that the Company's e-mail, Internet and/or intranet systems are to be used for conducting the Company's business only.

I have read the aforementioned document and agree to follow all policies and procedures that are set forth therein. I further accept the contents and agree to abide by the standards set in the document for the duration of my employment / contract with the Company.

I understand that the Company's need to implement this policy and agree to adhere thereto.

Employee's/ Contractor's Signature

Date

Employee's/ Contractor's Printed Full Name and Surname

Company Signature
(on behalf of the company)





B. Particulars of person on whose behalf request is made:

This section must ONLY be completed if a request for information is made on behalf of another person.

Full Names and Surname: _____

Identity Number:

--	--	--	--	--	--	--	--	--	--	--	--	--

C. Particulars of record:

- a) Provide full details of the record to which access is requested.
- b) If the provide space is inadequate, please continue on a separate page/ annexure and attach it to this form. The requested must sign all additional pages/ annexures.

Description of record or portion of the record requested:

2. Reference Number/ Heading (if Applicable):



3. Any further particulars of record:

Signed at _____, this day ____ of _____ year _____.

SIGNATURE OF REQUESTER / PERSON
ON WHOSE BEHALF REQUEST IS MADE

** This document remains the property of the company and may not be used, stored or copied without the written consent of the Information Officer.*

Document Prepared by: Q. Pelser

Document: SEES-POPI-2021-1-1

Revision: 0

FOR INTERNAL USE

Request received from: _____

Acting on Behalf of: _____ (if applicable)

Signature of Information Officer of the Company.



ANNEXE A

CONSENT FORM

DEFINITIONS:

1. "Signatory" - includes and not limited to an employee, agent, supplier and/or customer of the company.
2. "Company" - includes the entities as listed in the POPI Policy.

A. USE OF PERSONAL INFORMATION

1. The signatory, upon employment or registration or contractual engagement, signed an agreement incorporating a consent to process personal information for business and related purposes, including but not limited to conducting business.
2. Further to the above-mentioned agreement and consent, the Company hereby provide the following information with respect to processing the personal information or company information of the Signatory for purposes of employment or supplier or customer application, and the Signatory hereby provides the consent required by the Company for processing purposes.
3. The Company is committed to protecting the signatory's privacy and recognises that it needs to comply with statutory requirements in collecting, processing and distributing of personal information. The Constitution of the Republic of South Africa provides that everyone has the right to privacy and the Protection of Personal Information Act 4 of 2013 ("POPI") includes the right to protection against unlawful collection, retention, dissemination and use of personal information. In terms of section 18 of POPI, if personal information is collected, the Company, as responsible party, must take reasonably practical steps to ensure that the data subject is made aware of the information being collected.
4. In order to process employment, applications, contracts and agreements, it is necessary to provide potential third parties, namely: the Company's Accounting Officers, B-BBBEE rating agency, OHS agency, ISO certification agency and attorneys with personal information of the Signatory, which personal information includes, but are not necessarily limited to a Curriculum Vitae (CV), registration documents, contact details, identification numbers, financial information, registration numbers and duly authorised persons details.



This information is distributed to our accountants, B-BBBE rating agency, OHS agency, ISO agency and attorneys, usually by electronic means in the form of an email. This personal information to bursar / sponsors is necessary for purposes of contractual obligations.

5. In accordance with POPI, the Company hereby provides the following information:

5.1 Type of Information:

Information not necessarily limited to a Curriculum Vitae (CV), registration documents, financial information, contact details, identification numbers, registration numbers and dually authorised persons details.

5.2 Nature/category of Information:

Informative and Contractual for the purpose of conducting Business

5.3 Purpose:

5.3.1. Curriculum Vitae, ID and related information required by the employer for purposes of employing the employee in order to ensure the compliance with the Labour Act and Conditions of Employment Act.

5.3.2 Registration Documents (CIPC), Financial Documents and a Dually Authorised Person - for the purposes of contractual agreement between the Company and the Signatory for the purpose of conducting business as per the Companies Act and other legislation.

5.3.3 The Signatory is required to provide the information voluntarily and understands that same is mandatory for purposes of the employment or conducting business.



5.3.4 The Company may be required, directly or indirectly, in terms of legislation, (Such as the Labour Relations Act 66 of 1995 (as amended), The Basic Conditions of Employment Act 75 of 1997 (as amended)), and other statutes such as the Financial Intelligence Centre Act 38 of 2001, King 3 and 4 or similar statutes, to collect the information in order to report to the Ministry of Labour, Small Businesses or other Government structures and for responsible record keeping and statistical purposes.

5.3.5 The information is required in terms of the agreement between the signatory and the the Company.

5.3.6 Failure to provide the information will result in a failure to employ, retain employment or be captured as a supplier or customer with the Company in terms of the relevant regulations.

5.3.7. In giving references, The Company will NOT provide any reference of any kind to any other 3r party without the written consent of the Signatory. Such 3 rd party references do not form part of the consent given in this document.

6. The Signatory has the right to access and amend its personal information at any reasonable time.

7. The Signatory is entitled to object to the use of information. However, such objection may lead to the agreement being terminated as the information is required for valid reasons.

8. Complaints: All complaints regarding the use of personal information may be directed to the Information Officer, Mr. Q Pelser (quentin@simrox.co.za)



B. CONSENT

9. The Signatory (as data subject), by signing this document, hereby consents to the use of its personal information contained herein and confirms that:

9.1 the information is supplied voluntarily, without undue influence from any party and not under any duress;

9.2 the information which is supplied herewith is mandatory for the purposes of this agreement and that without such information, the Company will not enter into agreement with the Signatory;

10. The Signatory acknowledges that it is aware thereof that it has the following rights with regard to such personal information which is hereby collected. The right to:

10.1 access the information at any reasonable time for purposes of rectification thereof;

10.2 object to the processing of the information in which case this agreement will terminate in accordance with the provisions contained herein;

10.3 lodge a complaint to the Information Officer of the Company or The Information Regulator.

C. SIGNATORIES

Thus signed on this _____ day of _____ 20 ____ in the presence of the undersigned witnesses:

THE SIGNATORY:

Name and Surname: _____ ID: _____

(Dually Authorised)

if a Company also provide the Company Name and Registration Number:

WITNESSES:

1. _____ 2. _____

THE COMPANY

Thus signed on this _____ day of _____ 20 ____ in the presence of the undersigned witnesses:

On behalf of The Company: _____

(Mr. Q. Pelser - Information Officer)

WITNESSES:

1. _____ 2. _____