POLICY ON THE PROTECTION OF PERSONAL INFORMATION IN TERMS OF THE PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013 (POPIA)

For the purposes of this Policy unless otherwise noted, all references to [Umzimkhulu Industrial Holdings] (hereinafter referred to as the "**Company**") includes a reference to all the Company subsidiaries and associated companies.

1. INTRODUCTION

1.1. The Protection of Personal Information Act, 4 of 2013 ("**POPIA**") regulates and controls the processing of Personal Information.

1.2. The Company, for the purposes of carrying out its business and related objectives, does and will from time to time, processes the Personal Information of living individuals and legal entities including public and private entities, such as Personal Information pertaining to employees and staff, prospective employees and job applicants, students and interns, service providers and contractors, vendors, clients, tenants, and other third parties.

1.3. The Company is obligated to comply with POPIA and the data protection conditions housed under POPIA with respect to the processing of all and any Personal Information.

1.4. This Policy describes how the Company will discharge its duties in order to ensure continuing compliance with POPIA in general and the information protection conditions and rights of data subjects in particular.

2. DEFINITIONS

Please note the following definitions which will be used throughout this Policy and which are used under POPIA:

2.1. "**Biometrics**" means a technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition;

2.2. "**Child**" means a natural person under the age of 18 (eighteen) years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him-or herself;

2.3. **"Competent Person"** means any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child;

2.4. **"Consent"** means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of Personal Information;

2.5. **"Data Subject"** means the person to whom Personal Information relates;

2.6. **"Operator"** means a person who processes Personal Information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party;

2.7. **"Person"** means a natural person or a juristic person;

2.8. **"Personal Information"** means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to:

2.8.1. information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;

2.8.2. information relating to the education or the medical, financial, criminal or employment history of the person;

2.8.3. any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;

2.8.4. the biometric information of the person;

2.8.5. the personal opinions, views or preferences of the person;

2.8.6. 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;

2.8.7. the views or opinions of another individual about the person; and

2.8.8. the name of the person if it appears with other Personal Information relating to the person or if the disclosure of the name itself would reveal information about the person;

2.8.9. examples of Personal Information include:

2.8.9.1. a person's name and address (postal and email)

2.8.9.2. date of birth

2.8.9.3. statement of fact

2.8.9.4. any expression or opinion communicated about an individual

2.8.9.5. minutes of meetings, reports

2.8.9.6. emails, file notes, handwritten notes, sticky notes

2.8.9.7. photographs and CCTV footage if an individual can be identified by the footage

2.8.9.8. employment and student applications

2.8.9.9. spreadsheets and/or databases with any list of people set up by code or student/staff

2.8.9.10. employment number

2.8.9.11. employment or education history

2.8.10. special Personal Information includes:

2.8.10.1. any information relating to an individual's:

2.8.10.1.1. ethnicity

2.8.10.1.2. gender

2.8.10.1.3. religious or other beliefs

2.8.10.1.4. political opinions

2.8.10.1.5. membership of a trade union

2.8.10.1.6. sexual orientation

2.8.10.1.7. medical history

2.8.10.1.8. offences committed or alleged to have been committed by that individual

2.8.10.2. biometric details

2.8.10.3. children's details

2.9. **"Processing"** means any operation or activity or any set of operations, whether or not by automatic means, concerning Personal Information, including:

2.9.1. the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;

2.9.2. dissemination by means of transmission, distribution or making available in any other form; or

2.9.3. merging, linking, as well as restriction, degradation, erasure or destruction of information;

2.10. **"Public Record"** means a record that is accessible in the public domain and which is in the possession of or under the control of a public body, whether or not it was created by that public body;

2.11. **"Record"** means any recorded information:

2.11.1. regardless of form or medium, including any of the following:

2.11.1.1. writing on any material;

2.11.1.2. information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored;

2.11.1.3. label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;

2.11.1.4. book, map, plan, graph or drawing;

2.11.1.5. photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced;

2.11.2. in the possession or under the control of a responsible party;

2.11.3. whether or not it was created by a responsible party; and

2.11.4. regardless of when it came into existence;

2.12. **"Responsible Party"** means a public or private body or any other person who, alone or in conjunction with others, determines the purpose of and means for processing personal information;

2.13. **"User"** means the Person accessing, viewing or using the tools of the Company's website.

3. PURPOSE AND OBJECTIVES

3.1. This Policy sets out how the Company deals with Personal Information.

3.2. This Policy forms part of the Company's commitment to the safeguarding of Personal Information processed by it and its staff, Operators and or service providers.

3.3. The objective and purpose of this Policy is to:

3.3.1. set out the Company's policy on the processing of Personal Information;

3.3.2. ensure that all Company directors, executives, employees, and where applicable Company service providers, clients and Operators process Personal Information in accordance with POPIA and the POPIA conditions for the lawful processing of Personal Information;

3.3.3. provide a guideline to Company directors, executives, employees, and where applicable Company service providers, clients and Operators, on how the Company will process Personal Information.

3.4. This Policy is available on the Company website [www.rossmin.co.za] and on request from the Company's Information Officer.

4. THE DATA PROTECTION PRINCIPLES AND CONDITIONS

4.1. It is the duty of a Responsible Party and the Company to comply with all the data protection conditions set out under section 4 of POPIA, which are as follows:

4.1.1. Personal Information shall be obtained and processed fairly and lawfully;

4.1.2. Personal Information shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner

incompatible with that purpose or those purposes, unless specific consent to do so has been obtained;

4.1.3. Personal Information shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed;

4.1.4. Personal Information shall be accurate and, where necessary, kept up to date;

4.1.5. Personal Information processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes;

4.1.6. Personal Information shall be processed in accordance with the rights of data subjects under POPIA;

4.1.7. appropriate technical and organisational safeguards and measures must be put in place to protect and guard against unauthorised or unlawful processing of Personal Information and against accidental loss or destruction of, or damage to, personal data;

4.1.8. Personal Information shall not be transferred to another country unless that country or the person transferring the Personal Information ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

5. APPLICATION AND SCOPE

5.1. This Policy applies to all Personal Information processed by or on behalf of the Company and to the following persons:

5.1.1. all employees of the Company, who for the purposes of this Policy, means and will include all members of staff including permanent, fixed term, and temporary staff, directors and executives, secondees, agency workers, volunteers, interns, agents and sponsors engaged with the Company in South Africa, or overseas;

5.1.2. all employees employed by any of the Company's subsidiary or associated companies.

6. PERSONAL INFORMATION COLLECTED

6.1. The Company collects and processes Personal Information from a number of persons in order to carry out and pursue its business and related operational interests.

6.2. The type of Personal Information, which the Company processes, will depend on the need for which it is collected and will be processed for that purpose only.

6.3. Examples of Personal Information which the Company will from time to time collect includes but is not limited to:

6.3.1. the person's identity number, name, surname, address, postal code, marital status, and how many dependents they have;

6.3.2. the person's description of residence, business, assets; financial information, banking details;

6.3.3. the person's description of health, biometric details, expertise, qualification and skills;

6.3.4. any other information required by the Company or its service providers, and suppliers in order to provide an accurate analysis of that person's needs;

6.3.5. Information on a person's requirements, needs and specifications which is or may be used for marketing purposes to ensure that the Company products, services and offerings remain relevant and applicable;

6.3.6. further processing provided it is in line with the provisions of POPIA.

6.4. Upon request, any person, be it an employee or a person acting on behalf of the Company will provide each person from whom Personal Information is collected for the purpose of processing, a section 18 informed consent document.

7. HOW PERSONAL INFORMATION IS USED

The Company will only use a Person's Personal Information for the purpose for which it was collected and agreed. This may include:

7.1. recruitment and employment purposes;

7.2. conducting criminal reference checks;

7.3. entering into contracts, leases, sale agreements etc;

7.4. for risk assessments, insurance and underwriting purposes;

7.5. assessing and processing queries, enquiries, complaints, and / or claims;

7.6. conducting credit reference searches or verification;

7.7. confirming, verifying and updating persons details;

7.8. for purposes of personnel and other claims history;

7.9. for the detection and prevention of fraud, crime, money laundering or other malpractice;

7.10. conducting market or customer satisfaction research;

7.11. direct marketing purposes;

7.12. audit and record keeping purposes;

7.13. in connection with legal proceedings;

7.14. providing services to clients to carry out the services requested and to maintain and constantly improve the relationship;

7.15. providing communications in respect of the Company, its employees or other persons to governmental officials and regulatory agencies; and

7.16. in connection with and to comply with legal and regulatory requirements or when it is otherwise required or allowed by law.

8. INFORMED CONSENT

In accordance with POPIA, the Company, its employees and or Operators, will use its best endeavours, (save where it is unable to and this is due to it protecting the legitimate interests of the person whose Personal Information it is processing or the legitimate interests of the Company itself), only process Personal Information if the below mentioned conditions are met, which conditions are set out in the a section 18 informed consent document:

8.1. the person is told why the processing is necessary, what information is required and what will be done with it;

8.2. the person consents to the processing, which consent will be obtained at the time when that person's Personal Information is processed;

8.3. the processing is necessary i.e. in order to conduct an accurate analysis of that person's needs for purposes of amongst other employment reasons, credit limits, insurance requirements;

8.4. the processing is required as a result of or in order to comply with an obligation imposed by law on the Company;

8.5. the processing protects a legitimate interest of the Person and it is in the Person's best interest to have a full and proper needs analysis performed in order to provide them with an applicable and beneficial product or service;

8.6. processing is necessary for pursuing the legitimate interests of the Company or of a third party to whom the Personal Information is supplied.

9. DISCLOSURE AND SHARING OF PERSONAL INFORMATION

The Company may from time to time have to disclose certain Personal Information, which it has obtained from Persons to other parties, including its group of companies, subsidiaries or associated companies, joint venture companies and or approved product or third party service providers, regulators and or governmental officials, overseas service providers and related companies or agents, but such disclosure will always be subject to an agreement which will be concluded as between the Company and the party to who it is disclosing, which contractually obliges the recipient of the Personal Information to comply with strict confidentiality and data security conditions. A copy of this standard type agreement is available on request from the Information Officer.

10. SAFEGUARDING PERSONAL INFORMATION

10.1. All Company employees and where applicable, Operators and persons acting on behalf of the Company must before processing Personal Information ensure that the data will be kept secure and that appropriate measures and safeguards are in place to prevent any unauthorised access, disclosure and/or loss of such Personal Information.

10.2. Removing and Downloading Personal Information on to portable devices from workplace equipment or taking soft copies of Personal Information off-site must be

authorised in writing by the manager of the relevant department from where the information emanates and a copy of such authorisation sent to the Information Officer, and which removal will be subject to the following provisions:

10.2.1. the Person removing the Personal Information must explain and justify the operational need for the removal in relation to the volume and sensitivity of the Personal Information and ensure that the details of the Personal Information being removed is documented and recorded under a "**Removal Register**";

10.2.2. the Personal Information to be removed must be strongly encrypted;

10.2.3. the person removing and using said data should only store the data /necessary for their immediate needs and should remove the data as soon as possible once dealt with and such removal should be confirmed by way of a recordal in the Removal Register;

10.2.4. to avoid loss of encrypted data, or in case of failure of the encryption software, an unencrypted copy of the data must be held in a secure environment.

10.3. Where it is necessary to store Personal Information on portable devices such as laptops, USB flash drives, portable hard drives, CDs, DVDs, or any computer not owned by the Company all Company employees and where applicable, Operators and persons acting on behalf of the Company without exception must before storing said Personal Information ensure that the data is encrypted and is kept secure and that appropriate measures and safeguards are in place to prevent unauthorised access, disclosure and loss of such Personal Information and points 10.2.1 to 10.2.4 will apply to said data.

10.4. Where soft copies of Personal Information are removed from Company premises, all Company employees and where applicable, Operators and persons acting on behalf of the Company without exception must before removing said Personal Information ensure that only that data necessary for the purpose it is being removed is taken, is documented in a Removal Register and is thereafter whilst away form Company premises kept safe and secure and that appropriate measures and safeguards are in

place to prevent unauthorised access, disclosure and loss of such Personal Information .

10.5. Soft copies of Personal Information and portable electronic devices housing Personal Information should be stored in locked units, and they should not be left on desks overnight or in view of third parties.

10.6. Personal Information which is no longer required should be securely archived and retained, with consideration for the format and retention period requirements relating to the data and destroyed when no longer required, all to be done in line with the Company Records Management and Archive Policy and procedures.

10.7. Personal Information must not be disclosed unlawfully to any third party.

10.8. Transfers of Personal Information to third parties as per the provisions of clause 9, must be authorised in writing by the manager of the relevant department from where the information emanates and a copy of such authorisation sent to the Information Officer. Furthermore, such transfer must be protected by adequate contractual provisions or data processor agreements, as set out under clause 9 above.

10.9. All losses of Personal Information must be reported to the relevant manager of the department from where the information emanates, the departmental Data Protection Coordinator and the Information Officer.

10.10. Negligent loss or unauthorised disclosure of Personal Information, or failure to report such events, may be treated as a disciplinary matter.

10.11. The Company via its Information Security Officer and IT department will continuously review its security controls and processes to ensure that all Personal Information is secure.

11. ACCESS AND CORRECTION OF PERSONAL INFORMATION

11.1. Any person has the right to access their Personal Information which the Company holds about them, provided that they follow the right to access procedure set out under the Company's PAIA Manual.

11.2. Any person will also have the right to ask the Company to update, correct or delete their Personal Information on reasonable grounds by completing the relevant form found under the Company's PAIA Manual.

11.3. Any person has the right to object to the Company processing their Personal Information which the Company currently holds about them, by filing a notice of objection, which is found under the Company's PAIA Manual which can be obtained here, which objection must be brought to the attention of the Information Officer.

11.4. Once a Person objects to the processing of their Personal Information, the Company may no longer process said Personal Information.

11.5. The details of the Company Information Officer may be found in the Companies PAIA Manual.

12. RECORDS MANAGEMENT

12.1. Records in all formats containing Personal Information must be created, safely and securely stored and disposed of in accordance with the Company's Records Management and Archiving Policy and any associated procedures and codes of practice in place from time to time.

12.2. All records of Personal Information must be authentic, reliable and usable and capable of speedy and efficient retrieval.

12.3. All records of Personal Information must not be retained for periods longer than the periods permitted in the Company's retention schedule as per the Company's Records management and archiving Policy unless there is a specific reason there for and such retention is required for operational reasons.

13. ROLES AND RESPONSIBILITIES

Information Officer

13.1. The Company Information Officer has primary responsibility for the Company's compliance with POPIA. This comprises:

13.1.1. ensuring that the Company has a POPIA compliance program in place and that all employees and operators, service providers, contractors and agents acting for or on behalf of the Company are aware of this Policy and their obligations in relation to the POPIA compliance program;

13.1.2. maintaining the Company's notification with the Regulator;

13.1.3. handling data subject access requests and requests from third parties for Personal Information;

13.1.4. promoting and maintaining awareness of POPIA and regulations, including training;

13.1.5. investigating losses and unauthorised disclosures of personal Information.

Heads of Department / Division

13.2. The Company Heads of Department / Divisions are responsible for ensuring their employees and where applicable all operators, service providers, contractors and agents acting for or on behalf of the Company understand the role of the Information Protection conditions in their day-to-day work, through induction, training and performance monitoring, and for monitoring compliance within their own areas of responsibility.

Data Protection Coordinators

13.3. The Company Heads of Department / Divisions must ensure that Data Protection Coordinators are designated for their departments or divisions and provided with appropriate training and support. Coordinators are required to:

13.3.1. advise employees and where applicable Operators, service providers, contractors and agents acting for or on behalf of the Company in their

departments on the implementation of and compliance with POPIA and this Policy and any associated guidance / codes of practice;

13.3.2. ensure appropriate technical and organisational measures are taken within their departments to ensure against unauthorised or unlawful processing of Personal Information and against accidental loss or destruction of, or damage to, Personal Information;

13.3.3. support the Company's notification with the Regulator by maintaining the register of holdings of Personal Information, including databases and relevant filing systems, and the purposes of processing;

13.3.4. keep the Information Officer informed of changes in the collection, use, and security of Personal Information within their department;

13.3.5. report any loss of Personal Information to the Head of Department / Division and the Information Officer;

13.3.6. ensure the proper completion of all section 18 informed consent documents.

13.4. All the Company employees are responsible for:

13.4.1. processing Personal Information in accordance with POPIA, the POPIA conditions for processing, and any guidelines and instructions issued by the Company from time to time;

13.4.2. ensuring that they only process Personal Information, which is relevant and accurate and only for the purpose for which it is required;

13.4.3. ensuring that all special Personal Information will only be processed in line with the provisions set out under POPIA and in accordance with instructions set out by the Information Officer from time to time;

13.4.4. ensuring that all Personal Information and all records housing such Personal Information are safety retained, stored and archived and/ or destroyed when no longer required in accordance with the Company Records management and archiving Policy and procedures;

13.4.5. complying with all security and monitoring measures in order to safeguard and protect any Personal Information which he or she may be in possession of;

13.4.6. ensuring that any transfer of Personal Information to third parties is authorised, lawful and that appropriate and safe transport mechanisms are employed in respect of the Personal Information so transferred such as encryption;

13.4.7. ensuring that only authorised downloading of electronic Personal Information onto portable devices or the removal of manual Personal Information from Company premises occurs;

13.4.8. raising any concerns in respect of the processing of Personal Information with the Information Officer;

13.4.9. promptly passing on to the Information Officer all data subject access requests and requests from third parties for Personal Information;

13.4.10. reporting losses or unauthorised disclosures of Personal Information to the Information Officer;

13.4.11. ensure the Personal Information they provide about themselves is up to date;

13.4.12. not attempt to gain access to information that is not necessary to hold, know or process.

14. GENERAL

Any transgression of this Policy will be investigated and may lead to disciplinary action being taken against the offender.

15. ACCOUNT AND REGISTRATION DETAILS

15.1. To gain access to certain services on sites or apps, the User may be requested to create a User account by registering on the site. As part of the registration process, the User will be allocated a username and password.

15.2. The User agrees that the information supplied as required by the registration process will be truthful, accurate and complete, and undertakes to update the information as and when required.

15.3. Furthermore, the User agrees to not attempt to register in the name of any other individual, company or organisation, nor will the User adopt any username that is deemed to be offensive.

15.4. The User accepts full responsibility for all activities that occur under the User's access details or password and accepts responsibility for sharing the User's username and password.

15.5. The Company may refuse to provide products and/or services should the Company be unable to verify any information provided by the User.

15.6. The User agrees that the following actions shall constitute a material breach of these terms and conditions:

15.6.1. signing in as, or pretending to be another person;

15.6.2. transmitting material that violates, or could violate, the intellectual property rights of others or the privacy of others;

15.6.3. using interactive services in a way that is intended to harm, or could result in harm to the User or to other Users of the site; or

15.6.4. gathering information about others without obtaining their prior written consent.

15.7. The User agrees that any use of the User's access details shall be regarded as if the User were the person using such information.

15.8. The Company may determine certain requirements that the User will need to comply with when choosing a username or password. These requirements may be changed from time to time and the User may be required to update non-compliant credentials.

15.9. By providing the Company with the User's personal information as part of the registration process, the User consents to the storage and intended use (as communicated to the User) of such personal information by the Company and/or duly authorised agents.

15.10. All information supplied by the User as part of the registration process will be protected and used in accordance with the terms of the Company's privacy policy.

16. **INTELLECTUAL PROPERTY**

16.1. All content and data on this site, including, without limitation, trademarks, names, software, video, technology, logos, databases, know-how, text, graphics, icons, hyperlinks, personal information, designs, programs, publications, products, processes or ideas described in this site, are protected by copyright, trademark and other intellectual property rights owned by the Company or by third parties that have licensed or otherwise provided their material to the Company.

16.2. Unless expressly stated, all content and data on the site is protected by South African and international copyright laws.

16.3. The User may not modify the content in any way, nor delete any copyright or trademark notice.

16.4. The User is granted a limited, non-exclusive, non-assignable, revocable licence to use the content for personal use in accordance with the terms of use.

16.5. Nothing in these terms and conditions in any way confers on the User any licence or right under any trademarks, names or logos.

16.6. Except as expressly permitted by these terms and conditions, the User may not copy, reproduce, distribute, disassemble, decompile, reverse engineer, use for commercial purposes, repost on other sites, download, republish, transmit, display, adapt, alter, create derivative works from or otherwise extract, by way of "scraping" or otherwise, or re-utilise any of the content of the site or authorise any person, or procure any other person to do so.

16.7. The User may not cache any of the content for access by third parties, nor mirror or frame any of the content of the site, nor incorporate it into another site, or authorise or procure any other person to do so without our express written permission. If the User or any third party requires to establish a hyperlink, frame, metatag or similar reference ("**linking**") to this site, the Company's prior written consent is required. An application for linking must be submitted to the Information Officer.

16.8. The Company endeavours to ensure that adequate technology safeguards are employed to protect the information on the site. However, the Company cannot be held responsible for any consequences that may result from the unlawful breach of

copyright or unlawful dissemination of information by third parties copying information off the site.

17. **THIRD-PARTY LINKED SITES**

17.1. This site may contain content supplied by third parties, as well as certain images and links to other third-party sites ("**linked sites**").

17.2. Third-party content and linked sites are included solely for the convenience of the User and do not constitute any approval, endorsement or warranty by the Company.

17.3. The linked sites are not under the control of the Company and the Company is not responsible for the content of any linked site, including, without limitation, any link contained in a linked site, or any changes or updates to a linked site. Moreover, the Company is not responsible for the accuracy, completeness or reliability of third-party information. The User assumes sole responsibility for the use of third-party information.

17.4. The Company is not responsible for any form of transmission from linked sites, nor is the Company responsible for the access, functionality and availability of the site.

17.5. The User should be aware that if the User accesses a linked site, any personal information submitted on the resulting site will not be collected or controlled by the Company, and the User will be subject to the terms of use of this resulting site. From time to time the Company may employ the services of third parties to assist with the hosting and management of certain services and aspects of the Company site. the Company applies every effort to ensure that our sub-contractors comply with our privacy policy and widely accepted security standards and will be held accountable for any non-compliance.