POPIA
INTERNAL PRIVACY POLICY

PO-HR-21

REVISION: 1

PURPOSE AND SCOPE OF THIS POLICY -
The purpose of this Policy is to address how KSB complies fully with the data protection and privacy standards as set out in the Protection of Personal Information Act No. 4 of 2013 ("**POPIA**"); with regards to KSB's processing of the personal information of its employees and the obligations and requirements placed on KSB employees and relevant third party contractors (defined under this Policy) to maintain compliance with POPIA. In respect of KSB employees, this Policy forms part of the terms of employment of each KSB employee**.**

TABLE OF CONTENTS

1 INTRODUCTION

1.1 Through the conduct of its business activities, KSB (the "**Company**" / "**we**" / "**us**" / "**our**") processes (including collects, uses, stores, disseminates and disposes of) personal information of clients, suppliers, employees and/or other stakeholders (collectively, data subjects, as defined below).

1.2 KSB is committed to effectively managing personal information in accordance with the provisions of the Protection of Personal Information Act 4 of 2013 and any regulations promulgated pursuant thereto ("**POPIA**").

1.3 This privacy policy ("**Policy**") is intended to govern KSB's processing of personal information of its employees and to stipulate the obligations on employees and third party contractors in regard to their obligations to KSB where they are involved in the processing of personal information for KSB's business purposes.

2 DEFINITIONS

In this Policy, unless the context requires otherwise, the following words and expressions bear the meanings assigned to them and cognate expressions bear corresponding meanings –

2.1.1 "**child**" means a natural living person under the age of 18;

2.1.2 "**consent**" means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information;

2.1.3 "**data subject**" means a person to whom personal information relates;

2.1.4 "**de-identify**" means to delete any personal 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 and the term "**de-identified**" shall have a corresponding meaning;

2.1.5 "**direct marketing**" means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of: (i) promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or (ii) requesting the data subject to make a donation of any kind for any reason;

2.1.6 "**information officer**" means the person appointed by KSB as such, whose responsibility is to ensure the organisation's compliance with POPIA;

2.1.7 "**legitimate basis**" means any of the following legitimate bases recognised by POPIA for the processing of personal information –

2.1.7.1 the data subject, or a competent person where the data subject is a child, consents to the processing; or

2.1.7.2 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

2.1.7.3 the processing complies with an obligation imposed by law on the responsible party; or

2.1.7.4 the processing protects a legitimate interest of the data subject; or

2.1.7.5 the processing is necessary for pursuing the legitimate interests of KSB or of a third party to whom the information is supplied.

2.1.8 "**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 the responsible party;

2.1.9 "**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 –

2.1.9.1 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;

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

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

2.1.9.4 the biometric information of the person;

2.1.9.5 the personal opinions, views or preferences of the person;

2.1.9.6 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;

2.1.9.7 the views or opinions of another individual about the person; and

2.1.9.8 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;

2.1.10 "**Personnel**" has the meaning ascribed to such term in clause 4.1.1;

2.1.11 "**processing / process**" means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including –

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

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

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

2.1.12 "**Regulator**" means the Information Regulator established in terms of POPIA;

2.1.13 "**re-identify**" means, in relation to personal information of a data subject, to resurrect any information that has been de-identified that identifies the data subject, or can be used or manipulated by a reasonably foreseeable method to identify the data subject;

2.1.14 "**responsible party**" means a person or entity which, alone or in conjunction with others, determines the purpose of and means for processing of personal information and in most cases, this would be KSB; and

2.1.15 "**special personal information**" means personal information specifically relating to: (i) the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or (ii) the criminal behaviour of a data subject to the extent that such intimation relates to: (a) the alleged commission by a data subject of any offence; or (b) any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

3 PURPOSE

3.1 The purpose of this Policy is to describe KSB's processing of the personal information of its employees and to set out the obligations and requirements placed on KSB employees and relevant third party contractors (defined under this Policy) to maintain compliance with POPIA.

3.2 This Policy demonstrates KSB’s commitment to protecting the privacy rights of data subjects in the following manner –

3.2.1 through stating desired behaviour and directing compliance with the provisions of POPIA and best practices;

3.2.2 by developing and implementing internal controls for the purpose of managing the compliance risk associated with the processing of personal information;

3.2.3 by creating business practices that all Personnel are required to adhere to that will provide reasonable assurance that the rights of data subjects are protected and balanced with the legitimate interests KSB; and

3.2.4 by assigning specific duties and responsibilities to specific Personnel (including the information officer) to ensure compliance with POPIA in order to protect the interests of KSB and data subjects.

4 APPLICATION OF THIS POLICY

4.1 This Policy applies to –

4.1.1 all employees, directors, officers and other staff of KSB ("**Personnel**") and our protection of the personal information of such Personnel; and

4.1.2 all third parties who process the personal information of KSB's data subjects on behalf of KSB or as part of any functions or duties which they carry out (whether contractual or otherwise) including contractors, consultants, temporary employees or casual workers ("**Authorised Third Parties**").

4.2 This Policy is applicable to the processing of all personal information throughout the information life cycle within the KSB business operations and in respect of employee information, from the point of first collection of personal information until the time that such information is destroyed.

4.3 This Policy should be read in conjunction with all other relevant policies of KSB regulating privacy and protection of information.

4.4 This Policy will not apply to personal information which has been de-identified.

5 PROTECTION OF PERSONNEL PERSONAL INFORMATION

5.1 KSB must ensure that its data subjects (including clients, suppliers and other persons in respect of whom personal information is processed) are made aware of the rights conferred upon them as data subjects.

5.2 In carrying out its processing activities of Personnel, KSB will ensure that it gives effect to the following rights enshrined under POPIA –

5.2.1 <u>The right to access personal information</u>

KSB recognises that a data subject has the right to establish whether KSB holds personal information related to him, her or it, including the right to request access to that personal information, where such personal information is held by KSB.

5.2.2 <u>The right to have personal information corrected or deleted</u>

KSB recognises that a data subject has the right to request, where necessary, that his, her or its personal information must be corrected or deleted where KSB is no longer authorised to retain the personal information.

5.2.3 The right to object to the processing of personal information

KSB recognises that a data subject has the right, on reasonable grounds, to object to the processing of his, her or its personal information. In such circumstances KSB will give due consideration to the request and the requirements of POPIA.

5.2.4 The right to object to direct marketing

KSB recognises that a data subject has the right to object to the processing of his, her or its personal information for purposes of direct marketing.

5.2.5 The right to complain to the Regulator

KSB recognises that a data subject has the right to submit a complaint to the Regulator regarding an alleged infringement of any of the rights protected under POPIA and to institute civil proceedings regarding the alleged non-compliance with the protection of his, her or its personal information.

5.2.6 The right to be informed

KSB recognises that a data subject has the right to be notified that his, her or its personal information is being collected by KSB. The data subject also has the right to be notified in any situation where KSB has reasonable grounds to believe that the personal information of the data subject has been accessed or acquired by an unauthorised person.

5.3 KSB will only process Personnel personal information for the purposes associated with the employment of such Personnel and/or in respect of all related and ancillary processing activities flowing from the relevant employment, contractor or service provider relationship between the parties.

6 GENERAL GUIDING PRINCIPLES - PERSONNEL RESPONSIBILITY FOR PROCESSING OF PERSONAL INFORMATION

6.1 All Personnel and/or Authorised Third Parties must at all times be subject to, and act in accordance with, the following guiding principles in respect of any processing activities which they may be engaged in with regard to all personal information which they process on behalf of KSB and/or as part of their duties and responsibilities to KSB –

6.1.1 Accountability

6.1.1.1 KSB will ensure that the provisions of POPIA and the guiding principles outlined in this Policy are complied with through the encouragement of desired behaviour. However, KSB will take appropriate sanctions, which may include disciplinary action, against any Personnel who

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

6.1.1.2 Failing to comply with POPIA could potentially damage KSB's reputation, expose KSB to administrative fines or expose KSB to civil claims for damages. The protection of personal information is therefore the responsibility of all Personnel and Authorised Third Parties.

6.1.2 Processing Limitation

6.1.2.1 Personnel are required to ensure that KSB can comply with its obligation in regard to ensuring that personal information under its control is processed: (i) in a fair, lawful and non-excessive manner; (ii) in a transparent manner; (iii) only where a legitimate basis exists; and (iv) only for a specifically defined purpose.

6.1.2.2 KSB must inform the data subject(s) of the reasons for collecting his, her or its personal information and ensure that there is a legitimate basis prior to processing personal information. This may include having to obtain the consent of the data subject prior to processing personal information. If any Personnel or Authorised Third Parties' are unsure about whether there is a justifiable legal basis for processing personal information, please contact the information officer.

6.1.2.3 Where applicable, the data subject must be informed of the possibility that their personal information will be shared with third parties and/or affiliates of KSB and be provided with the reasons for doing so.

6.1.3 Purpose Specification

6.1.3.1 All of KSB's business units' and/or operations' processing must be informed by the principle of transparency.

6.1.3.2 Personnel need to ensure that they process personal information only for specific, explicitly defined and legitimate reasons and in such a manner so as to ensure that KSB at all times remains compliant with this obligation under POPIA. Where it is practical to do so, KSB must inform data subjects of these reasons prior to collecting or recording the data subject's personal information.

6.1.4 Further Processing Limitation

6.1.4.1 Personnel are to be aware that personal information must not be processed for a secondary purpose, unless that secondary purpose is compatible with the original purpose.

6.1.4.2 In this regard, further processing shall not be compatible with the purpose of collection if:

i. the data subject (or a competent person the case of a child's personal information) has consented to the further processing;

ii. the information has been deliberately made public by the data subject or is available in or derived from a public record;

iii. further processing is necessary to avoid prejudice to maintenance of the law by any public body;

iv. for compliance with an obligation under law generally or to enforce legislation concerning the collection of revenue;

v. for conduct of judicial proceedings;

vi. in the interests of national security;

vii. to prevent a serious and imminent threat to public health or safety or the life or health of the data subject or any other individual;

viii. or the personal information is used solely for historical, statistical or research purposes and the responsible party ensures that the personal information will not be published in an identifiable form;

ix. or the further processing is in accordance with an exemption granted by the Regulator in terms of POPIA. Therefore, where KSB seeks to process personal information 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, KSB must first obtain additional consent from the data subject.

6.1.5 Information Quality

6.1.5.1 KSB Personnel must take reasonable steps to ensure that all personal information collected is complete, accurate, not misleading and kept up to date. In this regard, KSB shall erase and rectify any inaccurate personal information.

6.1.5.2 Where personal information is collected or received from third parties, KSB must 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.

6.1.6 Openness

KSB Personnel must take reasonably practicable steps to ensure that the data subject is aware of the processing. POPIA requires KSB to disclose to the data subject certain information including the following: (i) what information is being processed; (ii) who has access to such information (e.g. whether the information will be transferred to any third parties, including third parties outside of the Republic of South Africa); (iii) the purposes of the processing; (iv) the legitimate interests pursued by KSB or by a third party where the processing is based on the legitimate interests ground; and (v) what the consequences will be should the data subject refuse to provide such information.

6.1.7 Security Safeguards

6.1.7.1 KSB will take all reasonable precautions, with regard to the nature of the personal information and the risks of the processing, to preserve the security of the personal information and, in particular, prevent its alteration, loss and damage, or access by non-authorised persons. POPIA requires KSB to ensure the security and integrity of personal information in its possession or under its control with appropriate, reasonable technical and organisational measures to prevent loss, unlawful access and unauthorised destruction of personal information. In this regard, when considering the measures to implement in order to safeguard the personal information, KSB shall take into account the nature, scope, context and purposes of the processing and the risk posed by the processing to the rights and freedoms of the data subjects.

6.1.7.2 KSB has put in place measures (having regard to generally accepted information security practices or industry specific requirements or professional rules) to identify internal and external security risks; maintain safeguards against such risks; regularly verify that the safeguards are effective and continually update safeguards in response to new risks.

6.1.7.3 KSB must ensure that all paper and electronic records comprising personal information are securely stored and made accessible only to authorised individuals.

6.1.7.4 Personnel are required to adhere to the requirements set out in this clause and to all relevant IT use, information security and physical security and safeguard policies and procedures, in force from time to time.

6.1.7.5 Confidentiality clauses should be included in all contracts with operators to reduce the risk of unauthorised disclosures of personal information for which KSB is responsible.

6.1.8 Data Subject Participation

In terms of POPIA, a data subject is entitled to request that its personal information is corrected, updated and deleted and KSB is required to take reasonably practicable steps to ensure that personal information is complete, accurate, not misleading and is updated from time to time to the extent that KSB is in possession of such information. In light of this, KSB must facilitate access to all personal information processed on request by a data subject.

7 PROCESSING OF SPECIAL PERSONAL INFORMATION

7.1 As part of the employment arrangement with KSB, KSB may be required to process special personal information of its Personnel. KSB will process such special personal information in accordance with the requirements of POPIA and will generally rely on one of the following bases on which to process such special personal information: (i) where the Personnel has given his/her/its express consent; or (ii) processing is necessary for the establishment, exercise or defence of a right or obligation in law; (iii) information has deliberately been made public by the Personnel; (iv) the processing of special personal information is for historical, statistical or research purposes to the extent that such purposes are: (a) in the public interest; or (b) it would have been impossible or disproportionate to ask for consent, and appropriate safeguards have been put in place to protect the personal information of the data subject.

7.2 KSB may be required to process special personal information as part of its normal business operations and if any Personnel are required to do so on KSB's behalf, they are obligated to ensure that any such processing is carried out in compliance with POPIA.

7.3 If you are unsure about whether any personal information constitutes special personal information and/or whether there is a legal basis for processing such special personal information, please contact the information officer.

7.4 KSB must only disclose special personal information to another person when –

7.4.1 the consent of the data subject has been obtained for such disclosure;

7.4.2 directed by an order of a court; and/or

7.4.3 required in terms of any applicable law.

7.5 KSB may not process any personal information concerning a child and will only do so where it has obtained the consent of the parent or guardian of that child or where KSB is permitted to do so in accordance with applicable laws.

8 COMPLIANCE WITH THE POLICY

8.1 The information officer is responsible for ensuring that this Policy is implemented throughout KSB.

8.2 The information officer is responsible for, *inter alia* –

8.2.1 taking steps to ensure KSB's reasonable compliance with the provisions of POPIA;

8.2.2 organising and overseeing the awareness training of Personnel and other individuals involved in the processing of personal information on behalf of KSB;

8.2.3 addressing any data breaches;

8.2.4 continually assessing KSB's personal information processing procedures and aligning them with applicable laws, privacy regulations and best practices. This will include reviewing KSB's information protection procedures and related policies from time to time. This Policy may be updated from time to time in line with this obligation;

8.2.5 ensuring that KSB makes it convenient for data subjects who want to update their personal information or submit POPIA related complaints to KSB. Personnel may contact the information officer on the details listed below;

8.2.6 approving any contracts entered into with Personnel and Authorised Third Parties. This will include overseeing the amendment of KSB's employment contracts and other data processing agreements, where applicable;

8.2.7 encouraging compliance with the conditions required for the lawful processing of personal information;

8.2.8 ensuring that Personnel and other persons acting on behalf of the organisation are fully aware of the risks associated with the processing of personal information and that they remain informed about the organisation's security controls;

8.2.9 addressing Personnel's and Authorised Third Party's POPIA related questions;

8.2.10 addressing all POPIA related requests and complaints made by Personnel and other data subjects; and

8.2.11 working with the Regulator in relation to any ongoing investigations.

9 PERSONNEL AND AUTHORISED THIRD PARTIES' OBLIGATIONS

9.1 Personnel and/or Authorised Third Parties may, during the course of the performance of their duties and/or services, gain access to and become acquainted with the personal information of certain employees, clients and suppliers of KSB.

9.2 Personnel and/or Authorised Third Parties are required to treat personal information as a confidential business asset of KSB and to respect the privacy of data subjects.

9.3 Personnel and/or Authorised Third Parties may not directly or indirectly, utilise, disclose or make public in any manner to any person or third party, either within KSB or externally, any personal information, unless such information is already publicly known or the disclosure is necessary in order for the relevant Personnel and/or Authorised Third Parties to perform his, her or its duties.

9.4 Personnel and/or Authorised Third Parties must request assistance from their line manager or the information officer if they are unsure about any aspect related to the protection of a data subject's personal information.

9.5 Personnel and/or Authorised Third Parties must only process personal information where a legitimate basis exists for such processing, bearing in mind that where special personal information is concerned, there are specific legitimate bases that apply for each type of special personal information. Personnel should request assistance in regard to the processing of special personal information from the information officer, where this is required.

9.6 Furthermore, personal information must only be processed where the data subject clearly understands why and for what purpose his, her or its personal information is being collected and processed.

9.7 Where the legal basis for processing is consent, Personnel and/or Authorised Third Parties must, prior to processing any personal information, obtain the data subject's consent.

9.8 Consent to process a data subject's personal information must be obtained directly from the data subject, except where exceptions apply, such as (*inter alia*) –

9.8.1 the personal information has been made public; or

9.8.2 where valid consent has been given to a third party; or

9.8.3 the information is necessary for effective law enforcement.

9.9 Personnel and/or Authorised Third Parties will under no circumstances –

9.9.1 process or have access to personal information where such processing or access is not a requirement to perform their respective work-related tasks or duties;

9.9.2 save copies of personal information directly to their own private computers, laptops or other mobile devices like tablets or smart phones;

9.9.3 share personal information through unsecure methods. Where access to personal information is required, this may be requested from the relevant line manager or the information officer; and

9.9.4 transfer personal information outside of the Republic of South Africa without the express permission from the information officer.

9.10 Personnel and/or Authorised Third Parties are responsible for –

9.10.1 keeping all personal information that they come into contact with secure, by taking sensible precautions and following the guidelines outlined within this Policy and any other applicable policies related to information security or record keeping;

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

9.10.3 where possible, ensuring that personal information is encrypted prior to sending or sharing the information electronically;

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

9.10.5 ensuring that their computer screens and other devices are switched off or locked when not in use or when away from their desks. Ensuring that where personal information is stored on removable storage medias such as external drives, flash sticks, CDs or DVDs that these are kept locked away securely when not being used;

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

9.10.7 ensuring that where personal information has been printed out, that the paper printouts are not left unattended where unauthorised individuals could see or copy them. For instance, close to the printer;

9.10.8 taking reasonable steps to ensure that personal information is kept accurate and up to date. For instance, confirming a data subject's contact details when the client or customer phones or communicates via email. Where a data subject's information is found to be out of date, authorisation must first be obtained from the relevant line manager or the information officer to update the information accordingly;

9.10.9 taking reasonable steps to ensure that personal information is stored only for as long as it is needed or required in terms of the purpose for which it was originally collected. Where personal information is no longer required, authorisation must first be obtained from the relevant line manager or the information officer to delete or dispose of the personal information in the appropriate manner and in accordance with KSB's Records Retention and Destruction Policy;

9.10.10 from time to time, undergoing POPIA awareness training, as may be required by KSB; and

9.10.11 where Personnel and/or Authorised Third Parties become aware or suspicious of any security breach such as the unauthorised access, interference, modification, destruction or the unsanctioned disclosure of personal information, he or she must immediately report this event or suspicion to the information officer.

9.11 Where necessary or appropriate, agreements with Authorised Third Parties to whom KSB may disclose personal information must be concluded to ensure that they process any personal information in accordance with the provisions of this Policy and POPIA. All such Authorised Third Parties should at the very least conclude non-disclosure agreements with KSB compelling them to secure and treat all personal information in their possession as confidential and preventing such third parties from disclosing such information.

9.12 All Authorised Third Parties who process data subject personal information must strictly adhere to the security requirements set forth in this Policy and to KSB's security policy(ies) and shall be required to maintain and where required, upgrade their systems and processes to comply with the terms of this Policy and such security policies.

9.13 KSB must carry out a due diligence of all Authorised Third Parties processing personal information on behalf of KSB and this may include auditing the facilities, security procedures and policies of such Authorised Third Parties.

9.14 Authorised Third Parties must immediately inform KSB (via the office of the information officer) of any actual or suspected security breach or compromise to personal information in its possession. The Authorised Third Parties may be required to notify the affected data subject(s) and the Regulator, but this should only be carried out on KSB's instructions, via the office of the information officer, and in accordance with KSB's Data Breach Response Plan.

10 REQUEST TO ACCESS PERSONAL INFORMATION PROCEDURE

10.1 Data subjects have the right to –

10.1.1 request information about personal information KSB holds about them and request reasons for holding it (including all information as set out in paragraph 5.2.1 above);

10.1.2 request access to their personal information. Access to such personal information can be requested by email, addressed to the information officer. The information officer will process all requests within a reasonable time; and

10.1.3 be informed how to keep their personal information up to date.

10.2 All requests for access received by KSB should be handled by the office of the information officer only and should any KSB Personnel member receive such a request, it should be immediately furnished to the office of the information officer and can be emailed to the inforequest.za@ksb.com

Personnel may also lodge any request for access to their own personal information with the information officer.

11 CROSS-BORDER TRANSFER OF PERSONAL INFORMATION

11.1 POPIA provides that KSB may not transfer personal information about a data subject to a third party in a foreign jurisdiction unless –

11.1.1 the recipient's country is subject to a law or the recipient is bound by a contract which –

11.1.1.1 upholds principles of reasonable processing of the information that are substantially similar to the principles contained in POPIA; and

11.1.1.2 includes provisions that are substantially similar to those contained in POPIA relating to the further transfer of personal information from the recipient to third parties; or

11.1.2 the data subject consents to the transfer; or

11.1.3 the transfer is necessary for the performance of a contract between the data subject and KSB, or for the implementation of pre-contractual measures taken in response to the data subject's request; or

11.1.4 the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the responsible party and a third party; or

11.1.5 the transfer is for the benefit of the data subject, and –

11.1.5.1 it is not reasonably practicable to obtain the consent of the data subject to that transfer; and

11.1.5.2 if it were reasonably practicable to obtain such consent, the data subject would be likely to give it.

11.2 In carrying out any cross-border transfers, KSB must adhere to the provisions of POPIA. For instance, KSB can send or transfer personal information of data subjects to KSB's group companies (where applicable) and/or Authorised Third Parties beyond the borders of the Republic of South Africa in order to achieve the purpose for which the personal information was collected and processed, including for processing and storage by Authorised Third Parties, if the applicable data subject(s) has consented to such cross-border transfer.

11.3 Any cross-border transfers of personal information should be brought to the attention of, and only be carried out after it has been authorised by, the information officer.

12 DATA STORAGE AND RETENTION

12.1 KSB and/or Authorised Third Parties must ensure that personal information, including special personal information and any commercially sensitive information which it processes is captured, used, disclosed, stored and destroyed in a secure and confidential manner appropriate to the classification of the information, in accordance with KSB's Data Retention and Destruction Policy, the relevant provisions of POPIA, and other applicable laws.

12.2 Authorised Third Parties, including data storage and processing providers, may from time to time also have access to a data subject's personal information in connection with the storage and retention thereof. KSB must ensure that these Authorised Third Parties only process the personal information in accordance with the provisions of this Policy, all other relevant internal policies of KSB and POPIA.

12.3 In order to comply with POPIA, KSB must –

12.3.1 keep records of the personal information it has collected, correspondence or comments in an electronic or hardcopy file format. Personal information may be processed for as long as necessary to fulfil the purposes for which that personal information was collected and/or as permitted or required by applicable law;

12.3.2 retain personal information for longer periods for statistical, historical or research purposes, and should this occur, KSB must ensure that appropriate safeguards have been put in place to ensure that all recorded personal information will continue to be processed in accordance with this Policy and the applicable laws; and

12.3.3 once the purpose for which the personal information was initially collected and processed no longer applies or becomes obsolete, ensure that it is deleted, destroyed or de-identified so that a third party cannot re-identify such personal information.

13 PROCESSING OF PERSONAL INFORMATION OF PERSONNEL

13.1 KSB's human resource function ("**HR**") shall ensure that they comply with this Policy in respect of all KSB's Personnel data which they have on file and collect and which falls within the definition of personal information, including that HR will only collect such personal information of Personnel as is necessary for their employment relationship with KSB. This includes information collected from the time that a potential member of Personnel applies for a job, during the interview and selection process and if such candidate is successful, all information processed during the course of their employment and on the termination of their employment.

13.2 For clarity, it is recorded that KSB shall not process personal information of Personnel without first obtaining Personnel consent to such processing or ensuring that it can rely on the existence of an alternate legitimate basis.

14 COMPLAINTS PROCEDURE

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

14.1.1 Complaints in terms of POPIA must be submitted to KSB (for the attention of the information officer) in writing as follows –

by post: PO BOX 2938, PRIMROSE, 1416; and/or by e-mail: inforequest.za@ksb.com

14.1.2 Where the complaint has been received by any person other than the information officer, that person will ensure that the full details of the complaint reach the information officer within 7 working days.

14.1.3 The information officer will provide the complainant with a written acknowledgement of receipt of the complaint within 14 working days and consider and address the complaint in an appropriate manner and in accordance with the principles outlined in POPIA.

14.1.4 The information officer will revert to the complainant with a proposed solution with the option of escalating the complaint to KSB's Senior Management within 21 working days of receipt of the complaint. In all instances, KSB will provide reasons for any decisions taken and communicate any anticipated deviation from the specified timelines.

14.1.5 Where the data subject is not satisfied with the information officer's suggested remedies, the data subject has the right to complain to the Regulator. The website of the Regulator can be accessed at the following link: **http://justice.gov.za/inforeg/**.

14.1.6 Where the information officer has reason to believe that a data breach has occurred and any personal information of data subjects has been unlawfully accessed or acquired by an unauthorised person, the information officer will consult with KSB's Senior Management, where after the affected data subjects and the Regulator will be informed of the breach in accordance with the provisions of POPIA and KSB's Data Breach Response Policy.

15 ENFORCEMENT AND REPORTING OF BREACHES OF THIS POLICY

15.1 Any non-compliance with the terms of this Policy could have serious legal and reputational repercussions for KSB and my cause significant damage to KSB. Therefore, any noncompliance could lead to disciplinary action being taken against the relevant employees.

15.2 Should any employee become aware of any noncompliance with the terms of this Policy, they are required to immediately report this to their relevant line managers, who in turn should report this to the information officer. Such reports may also be sent to the following email address: inforequest.za@ksb.com

16 EFFECTIVE DATE AND POLICY REVIEW

16.1 This Policy is effective from 1 January 2021

This Policy will be reviewed at regular intervals when appropriate, to ensure that it deals appropriately with KSB's processing of personal information. Any changes to this Policy must be approved by the information officer.