Policy:

Protection of Personal Information

Revision Number: 00

Issue Date: 15 February 2021

Signed by: _____

Chairperson

Conforms to ISO 9001:2015

Table of Contents

1. PURPOSE

The purpose of this policy is aligning the Company's role in protecting personal information with the Protection of Personal Information Act, 2013 by-

a) Giving effect to the constitutional right to privacy, by safeguarding personal information when processed by the Company, subject to justifiable limitations that are aimed at:

   i) balancing the right to privacy against other rights, particularly the right of access to information;
   ii) protecting important interests, including free flow of information within the Republic and across international borders.

b) Regulate the way personal information may be processed, by establishing conditions, in harmony with international standards, that prescribe the minimum threshold required for lawful processing or personal information.

c) Provide persons with rights and remedies to protect their personal information from processing that is not in accordance with the Act.

d) Establish voluntary and compulsory measures to enforce and fulfil the rights protected by the Act

2. REVISIONS AND UPDATING SCHEDULE

a) The policy needs to be reviewed and updated annually.

3. DEFINITIONS / GLOSSARY

Biometrics	Means a technique of personal identification that is based on physical, physiological, or behavioral characterization including blood typing, fingerprinting, DNA analysis, retinal scanning, and voice recognition.
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.
Consent	Means any voluntary, specific, and informed expression of will in term of which permission is given for the processing of personal information.
Data Subject	Means the person to whom personal information relates. This will include employees, customers, website users, contractors, and students.

De-identify	in relation to personal information of a data subject, means to delete any information that- a) identifies the data subject. b) can be used or manipulated by a reasonably foreseeable method to identify the data subject. c) can be linked by a reasonably foreseeable method to other information that identifies the data subject.
Direct marketing	Means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of- a) promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject. b) requesting the data subject to donate any kind for any reason.
Electronic Communication	Means any text, voice, sound, or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient.
Enforcement notice	Means notice issued in terms of section 95 of Act No. 4 2013
Filing System	Means any structure set of personal information, weather centralized, decentralized, or dispersed on a functional or geographical basis, which is accessible according to specific criteria.
Personal Information	Means information relating to an identifiable, living, natural person and where it is applicable, and identifiable, existing juristic person, including, but not limited to- a) information relating to the race, gender, sex, pregnancy, marital status, national, ethical, or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language, and birth of the person. b) information relating to the education or medical, financial, criminal or employment history of the person. c) any identifying number, symbol, email address, physical address, telephone number, location information, online identifier, or other assignment to the person. d) the biometric information to the person.

e) the personal opinions, views, or preferences of the person

f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature of further correspondence that would reveal the contents of the original correspondence.

g) the views or opinion of another individual about the person.

h) 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.

Processing Means any operation or activity or any set of operations, whether automatic, concerning personal information including-

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

b) dissemination by means of transmission, distribution or making available in any other form.

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

Record Means any recorded information-

a) regardless of form of medium, including any of the following:

i. writing on any material
ii. information produced, recorded, or stored by means of any type of recorder, computer equipment, whether hardware or software or both, or other device and any material subsequently derived from information so produced, recorded, or stored.
iii. label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means.
iv. book, map, plan, graph, or drawing
v. photograph, film, negative, tape or other device in which one or more visual images are embodied to be capable, with or without the aid of some other equipment, of being reproduced.

b) in the possession or under the control of a responsible party.

c) Whether or not it was created by a responsible party.

d) Regardless of then it came into existence.

Re-identify in relation to personal information of a data subject, means to resurrect any information that has been de-identified, that-

a) Identifies the data subject.

b) can be used or manipulate by a reasonably foreseeable method to identify the data subject.

c) can be linked by a reasonably foreseeable method to other information that identifies the data subject.

Unique identifier Means any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party.

4. APPLICATION AND INTERPRETATION

4.1 This policy applies to the processing for personal information-

4.1.1 Entered in a record by or for the Company by making use of automated or non-automated means, provided that when the recorded personal information is processed by non-automated means, it forms part of a filing system or is intended to form part thereof.

4.1.2 If any other legislation provides for conditions for lawful processing of personal information that are more extensive than those set out in this policy, the extensive condition prevails.

4.2 Rights of data subjects (which includes employees and non-employees)

A data subject had the right to have his/her personal information processed in accordance with the conditions for lawful processing of personal information, including the right –

(a) to be notified that -

(i) personal information about him or her is being collected
(ii) his/her personal information has been accessed or acquired by an unauthorised person

(b) to establish if the Company holds personal information and to request access to his/her personal information.

(c) to request, where necessary, the correction, destruction, or deletion of his/her personal information.

(d) to object, on reasonable grounds relating to his/her situation, to the processing of his/her personal information.

(e) to object to the processing of his/her personal information at any time for the purpose of direct marketing.

(f) not have his/her personal information processed for the purpose of direct marketing by means of unsolicited electronic communications.

(g) to submit a complaint to the Regulator regarding the alleged interference with the protection of the subject's personal information or to submit a complaint to the Regulator in respect of determination of an adjudicator.

5. CONDITIONS FOR LAWFUL PROCESSING OF PERSONAL INFORMATION

5.1 Processing of personal information in general

5.1.1 Condition 1 - Accountability

a) The Company must ensure that the conditions set out in this section, and all the measures that give effect to such conditions, are complied with at the time of the determination of the purpose and means of the processing and during the processing itself.

5.1.2 Condition 2 - Processing limitation

5.1.2.1 Lawfulness of processing

Personal information must be processed –

(a) lawfully and-
(b) in a responsible manner that does not infringe on the privacy of the data subject.

5.1.2.2 Minimality

Personal information may only be processed if, given the purpose for which it is processed, is adequate, relevant, and not excessive.

5.1.2.3 Consent, justification, and objection

Personal information may only be processed if –

(a) the data subject consents to the processing.
(b) processing is necessary to carry out actions for the conclusion of performance of a contract to which the data subject is party.
(c) processing complies with an obligation imposed by law on the Company.
(d) processing protects a legitimate interest of the data subject.
(e) processing is necessary for the proper performance of a public law duty by a public body; or
(f) processing is necessary for the pursuing legitimate interests of the Company or third party to whom the information is supplied.

The Company bears the burden of proof of the data subject's consent. The data subject may withdraw his/her consent at any time, provided that the lawfulness of the processing of personal information will not be affected.

The data subject my object, at any time, to the processing of personal information -

(a) in terms of processing that:

(i) protects a legitimate interest of the data subject;

(ii) is necessary for the pursuing legitimate interests of the Company or third party to whom the information is supplied, in the prescribed manner, on reasonable grounds relating to his/her situation, unless legislation provides for such processing or for the purpose of direct marketing by means of unsolicited electronic communications.

If a data subject has objected to the processing of personal information, the Company may no longer process the personal information.

5.1.2.3 Collection directly from data subject

Personal information must be collected directly from the data subject, except if –

(a) the information is contained in or derived from a public record or has deliberately been made public by the data subject.
(b) the data subject has consented to the collection of the information from another source.
(c) collection of the information from another source would not prejudice a legitimate interest of the data subject.
(d) collection of the information from another source is necessary:

(i) to avoid prejudice to the maintenance of the law by any public body

(ii) to comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Service Act, 1997 (Act No. 34 of 1997)

(iii) for the conduct of proceedings in any court that are reasonably contemplated

(e) compliance would prejudice a lawful purpose of the collection or;

(f) compliance is not reasonably practicable in the circumstances of the case.

5.1.3 Condition 3 - Purpose specific

5.1.3.1 Collection for a specific purpose

Personal information must be collected for a specific, explicitly defined, and lawful purpose related to a function or activity of the Company. Each HOD needs to keep an updated record of what information is collected and why. This record should be available to a data subject on request.

5.1.3.2 Retention and restriction of records

Records of personal information must not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed, unless-

(a) retention of records is required or authorised by law;
(b) the Company reasonably requires the record for lawful purposes related to its functions or activities;
(c) retention of the record is required by a contract between the Company and data subject;
(d) the data subject has consented to the retention of the record

Records of personal information may be retained for periods in excess of those contemplated above, for historical, statistical or research purposes if the Company has established appropriate safeguards against the records being used for other purposes.

The Company must destroy or delete a record of personal information or de-identify it as soon as it is no longer authorised to retain the record. The destruction or deletion of a record of personal information must be done in a manner that prevents its reconstruction in an intelligible form.

The Company must restrict processing of personal information if-

(a) its accuracy is contested by the data subject, for a period enabling the Company to verify the accuracy of the information.
(b) the Company no longer needs the personal information for achieving the purpose for which the information was collected.

5.1.4 Condition 4 - Information quality

The Company must take reasonably practicable steps to ensure that the personal information is complete, accurate, not misleading and updated where necessary. The Company must have regard for the purpose for which personal information is collected or processed.

5.1.5 Condition 5 - Openness

5.1.5.1 Documentation

The Company must maintain the documentation of all processing operations under its responsibility as referred to in section 14 or 51 of the Promotion of Access of Information Act.

5.1.5.2 Notification to data subject when collecting personal information

When personal information is collected, the Company must take reasonably practicable steps to ensure that the data subject is aware of-

(a) the information being collected and where the information is not collected from the data subject, the source which it is collected.
(b) the purpose for which the information is being collected.
(c) whether or not the supply of the information by the data subject is voluntary or mandatory.
(d) the consequences of failure to provide information.
(e) any law authorizing or requiring the collection of the information.
(f) the fact that, where applicable, the Company intends to transfer the information to a third party and the level of protection afforded to the information by the third party.
(g) existence of the right of access to and the right to rectify the information collected.
(h) existence of the right to object to the processing of personal information
(i) existence of the right to lodge a complaint to the Information Regulator and contact details of the Information Regulator.

5.1.6 Condition 6 - Security Safeguards

5.1.6.1 Security measures on integrity and confidentiality of personal information

The Company must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent-

(a) loss of, damage to or unauthorised destruction of personal information; and
(b) unlawful access to or processing of personal information.

To affect the above, the Company must take reasonable measures to-

(a) identify all reasonably foreseeable internal and external risks to personal information in its posse ssion or under its control.
(b) establish and maintain appropriate safeguards against the risks identified.
(c) regularly verify that the safeguards are effectively implemented; and
(d) ensure that the safeguards are continually updated in response to new risks or def iciencies, in previously implemented, safeguards.

The Company must have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations.

Information processed and security measures regarding information processed by an operator or person acting under authority.

Any employee processing personal information on behalf of the Company must-

(a) only do so with the knowledge or authorisation of the Company
(b) treat personal information which comes to their knowledge, as confidential and must not disclose it, unless required by law or during the proper performance of their duties.
(c) notify the Company immediately where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person.

The Company must, in terms of a written contract between the Company and the employee, ensure that the employee who processes personal information for the Company maintains the security measures above.

5.1.6.2 Notification of security compromise

Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, the Company must notify the data subject. The notification must be made as soon as reasonably possible after the discovery of the compromise.

The Company may only delay notification to the data subject if the notification will impede a criminal investigation by a public body.

The notification must be in writing and communicated to the data subject in at least one of the following ways-

(a) mailed to the data subjects last know physical address.
(b) sent by e-mail to the data subject's last known e-mail address.

(c) placed in a prominent position on the Company's website.
(d) published in the news media.

The notification must provide sufficient information to allow the data subject to take protective measures against potential consequences of the compromise, including-

(a) a description of the possible consequences of the security compromise.
(b) a description of the measures the Company intends to take or has taken to address the security compromise.
(c) a recommendation about the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise.
(d) if known to the Company, the identity of the unauthorised person who may have access or acquired the personal information.

5.1.7 Condition 7 - Data subject participation

5.1.7.1 Access to personal information

A data subject, having provided adequate proof of identity, has the right to-

(a) request the Company whether the Company holds personal information about the data subject.
(b) request from the Company a record or a description of the personal information held within a reasonable time, in a reasonable manner and format and in a form that is generally understandable.

In response to a request for personal information from a data subject, the data subject must be advised of the right to request the correction of information.

5.1.7.2 Correction of personal information

A data subject may request the Company to correct or delete personal information that is in its possession or under its control that is inaccurate, incomplete, excessive, out of date, irrelevant, misleading, or obtained unlawfully.

5.1.8 Processing of special personal information

5.1.8.1 Prohibition on processing of special personal information

The Company may not process personal information concerning-

(a) religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health, or biometric information of a data subject; or

(b) criminal behaviour of a data subject to the extent that such information relates to alleged commission of any offence or any proceedings in respect of any offence allegedly committed.

The prohibition does not apply to-

(a) processing carried out with the consent of the data subject.
(b) processing is necessary for the establishment, exercise, or defense of a right or obligation in law.
(c) processing is necessary to comply with an obligation of international public law.
(d) processing if for historical, statistical or research purposes to the extent that:

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

(e) information had deliberately been made public by the data subject.

5.1.8.2 Authorisation concerning a data subject's race or ethnic origin.

The prohibition on processing personal information concerning a data subject's race or ethnic origin does not apply if the processing is carried out to-

(a) identify the data subject and only when this is essential for that purpose; and
(b) comply with laws and other measures designed to protect or advance persons, or categories of persons, disadvantaged by unfair discrimination.

5.1.8.3 Authorisation concerning a data subject's biometric information.

The processing of information concerning employees must take place in accordance with the rules and regulations of the Company's HR policy and in compliance with labour legislation.

5.1.8.4 Processing of personal information of children

The Company may not process personal information concerning children.

6. RIGHTS OF A DATA SUBJECT REGARDING DIRECT MARKETING

6.1 Direct marketing by means of unsolicited electronic communications.

The processing of personal information of a data subject for the purposes of direct marketing by means of any form of electronic communication including SMSs and e-mail is prohibited unless the data subject-

(a) has given his/her consent to the processing; or
(b) is a customer of the Company?

The Company may approach a data subject whose consent is required and who has not previously withheld such consent.

Any communication for the purpose of direct marketing must contain -

(a) details of the identity of the sender
(b) an address or other contact details to which the recipient may send a request that such communication cease.

7. TRANSBORDER INFORMATION FLOWS

The Company may not transfer personal information about a data subject to a third party who is in a foreign country unless-

(a) the third party receiving the information is subject by law, binding corporate rules or binding agreement which provide adequate level of protection.
(b) the data subject consents to the transfer.
(c) the transfer is necessary for the performance or conclusion of a contract between the parties.
(d) the transfer is for the benefit of the data subject.

8. NON-COMPLIANCE WITH THE CONFLICT-OF-INTEREST POLICY

Non-compliance with this policy and the procedures associated with it may result in disciplinary action and even dismissal. Head of Departments and Executive management must ensure that all Kishugu employees in their areas of responsibility are aware of and understand Kishugu's Protection of Personal Information Policy.

REVISION HISTORY AND APPROVAL

Revision History: This document is reviewed to ensure its continuing relevance to the systems and process that it describes. A record of contextual additions or omissions is given below:

Rev No:	***Date:***	***Revised By:***	***Reason for Revision***
00	15 February 2021		Original. New Policy approved by Kishugu Holdings Board.