



**MARIAKANI MABATI SACCO SOCIETY
LIMITED**

DATA PROTECTION POLICY
©2024

TABLE OF CONTENTS

Contents

ABBREVIATIONS AND ACRONYMS	4
DEFINITION OF TERMS	5
<i>Data Protection Impact Assessment</i>	5
<i>Data Protection Officer</i>	6
<i>Personal Data Breach</i>	6
1.0 INTRODUCTION	7
1.1 <i>Purpose of this Policy</i>	7
1.2 <i>Scope of this Policy</i>	7
1.3 <i>Registration with the Office of the Data Protection Commissioner</i>	8
2.0 PERSONAL INFORMATION MANAGEMENT	9
2.1 <i>Justification for collection of personal information</i>	9
2.2 <i>Sources of personal information</i>	9
2.3 <i>Forms of personal information collected</i>	10
2.4 <i>Personal Data Protection Principles</i>	11
2.4.1 <i>Fairness and lawfulness</i>	11
2.4.2 <i>Restriction to a specific purpose</i>	12
2.4.3 <i>Transparency</i>	12
2.4.4 <i>Data reduction and data economy</i>	12
2.4.5 <i>Deletion</i>	12
2.4.6 <i>Factual accuracy; up-to-date data</i>	12
2.4.7 <i>Confidentiality and data security</i>	13
2.5 <i>Rights of the Data Subject</i>	13
2.6 <i>Data Subject Consent</i>	13
2.7 <i>Confidentiality of Data Processing</i>	15
2.8 <i>Data Processing Security</i>	15
2.9 <i>Duration for holding personal information</i>	16
2.10 <i>Data Breach and Notification</i>	16
2.10.1 <i>Notification to the ODPC</i>	16
3.1 <i>Organizational responsibilities</i>	16
3.1.2 <i>Data Protection Impact Assessment (Privacy Assessment)</i>	16
3.2 <i>Data Protection Officer Responsibilities</i>	17
3.3 <i>Staff responsibilities</i>	17
3.4 <i>Third-Party Data Processors</i>	18
3.5 <i>Contractors and Temporary Staff</i>	19

3.0 COMPLIANCE 19

POLICY REVISION..... 21

ADOPTION OF POLICY 21

APPENDIX I: OATH OF CONFIDENTIALITY/SECREC.....22

APPENDIX II: THIRD PARTIES/PARTNERS’ NON-DISCLOSURE AGREEMENT.....23

ABBREVIATIONS AND ACRONYMS

BOD	–	Board of Directors
CEO	–	Chief Executive Officer
CRB	–	Credit Reference Bureau
DPIA	–	Data Protection Impact Assessment
DPO	–	Data Protection Officer
ODPC	–	Office of Data Protection Commissioner
EACC	–	Ethics and Anti-Corruption Commission
ICT	–	Information and Communication Technology
ID	–	Identification
NHIF	–	National Hospital Insurance Fund
NSSF	–	National Social Security Fund
SASRA	–	Sacco Societies Regulatory Authority
SLA	–	Service Level Agreement

DEFINITION OF TERMS

Anonymization	The removal of personal identifiers from personal data so that the data subject is no longer identifiable.
Biometric data	Personal data resulting from specific technical processing based on physical, physiological or behavioral characterization including blood typing, fingerprinting, deoxyribonucleic acid analysis, earlobe geometry, retinal scanning and voice recognition.
Consent	Agreement which must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the processing of personal data relating to them.
Data	Information which is processed by means of equipment operating automatically in response to instructions given for that purpose or recorded with intention that it should be processed by means of such equipment or recorded as part of a relevant filing system.
Data Controller	The person or organization that determines when, why and how to process personal data. It is responsible for establishing practices and policies in accordance with the Data Protection Act. Mariakani Mabati Sacco is the Data Controller of all personal data relating to it and used in facilitating its business operations.
Data Processing	Any activity that involves the use of personal data and includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organizing, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties. In brief, it is anything that can be done to personal data from its creation to its destruction, including both creation and destruction.
Data Protection Impact Assessment	This is a tool or procedure of identifying and reducing risks involved in any processing activity that will involve personal data.

Data Protection Officer	The person appointed as such under the Data Protection Act and in accordance with its requirements. A data protection officer is responsible for advising the Sacco (including employees) on their obligations under various data protection laws, for monitoring compliance with data protection law, as well as with Mariakani Mabati Sacco policies.
Data Subject	A living, identified or identifiable individual about whom the Sacco holds personal data.
Personal Data	Any information identifying a data subject or information relating to a data subject that the Sacco can identify (directly or indirectly) from that data alone or in combination with other identifiers the Sacco possess or can reasonably access. Personal data includes sensitive personal data and pseudonymized personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth, gender) or an opinion about that person's actions or behavior.
Personal Data Breach	Any breach of security resulting in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to, personal data, where that breach results in a risk to the data subject.
Profiling	Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, to analyze or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements. Profiling is an example of automated processing.
Third Party	Any natural or legal person other than the data subject, Mariakani Mabati Sacco, or any implementing partner.

1.0 INTRODUCTION

1.1 Purpose of this Policy

This Data Protection Policy has been developed as a guide to Mariakani Mabati Sacco in management of stakeholders' data. Mariakani Mabati Sacco obtains, uses, stores and otherwise processes personal data relating to its stakeholders such as potential and current employees, former staff, members, suppliers, visitors to Sacco premises, contractors and website users, collectively referred to in this policy as data subjects. This Policy sets out how the Sacco manages those responsibilities.

In developing this Policy, the BOD intended to have this as the primary reference point for all matters pertaining to data management in the Sacco. Contents of this Policy was therefore carefully studied and implemented, as it constitutes an integral part of the Society's risk management processes.

The Sacco heavily draws its data policy guidelines from the Data Protection Act, 2019 and the Data Protection General Regulations, 2021. When processing personal data, the Sacco is obliged to fulfil individuals' reasonable expectations of privacy by complying with the Act and related Regulations and other relevant data protection legislation.

The policy document is therefore intended to ensure that the Sacco:

- Is clear about how personal data must be processed and the Sacco's expectations for all those who process personal data on its behalf.
- Complies with existing data protection laws and with good practice.
- Protects its reputation by ensuring the personal data entrusted to it is processed in accordance with data subjects' rights.
- Protects itself from risks of personal data breaches and other breaches of data protection law.

1.2 Scope of this Policy

This policy applies to all personal data the Sacco processes regardless of the location where that personal data is stored (e.g. on an employee's own device, Mariakani Mabati Sacco's

servers, Sacco website, cloud provider's servers, etc.) and regardless of the data subject. All staff and other parties processing personal data on Mariakani Mabati Sacco's behalf must read and comply with the provisions of this Policy. Failure to comply with this policy may result in disciplinary action.

The Sacco board of directors and staff are responsible for ensuring that they comply with this policy and should implement appropriate practices, processes, controls, and training to ensure that compliance. The Chief Executive Officer is responsible for overseeing this policy.

13 Registration with the Office of the Data Protection Commissioner

The Sacco shall register with the Office of the Data Protection Commissioner as a data controller and processor in accordance with the Data Protection Act and Regulations thereof.

2.0 PERSONAL INFORMATION MANAGEMENT

2.1 Justification for collection of personal information

The Sacco may collect and use Data Subject's personal data:

- If it is necessary for the Sacco's legitimate interest and so long as its use is fair, balanced and does not unduly impact data subject's rights.
- With the Data Subject's consent. For example, to send marketing emails, to take and use a data subject's photograph, to collect relevant medical information. The data subject can withdraw consent for this at any time.
- As required to fulfil the Sacco's legal obligations as a registered Deposit Taking Co-operative Society and employer. This includes sharing personal info with bodies such as SASRA, Ministry responsible for co-operatives, NSSF, NHIF, Courts, Police, EACC, CRBs, among other legal/statutory bodies.

The Sacco will only process sensitive personal data if it has data subject's explicit consent. In extreme situations, the Sacco may share data subject's personal details with the emergency services if it believes it is in data subject's 'vital interests' to do so.

2.2 Sources of personal information

The Sacco may collect information about data subject from different sources, for example:

- i. Directly from data subject when they:
 - Apply for membership
 - Apply for account opening
 - Apply for Sacco loan products
 - Apply for employment/internship
 - Are employed in the Sacco
 - Apply as a supplier
 - Register for or at one of the Sacco's events
 - Complete a survey
 - Subscribe for updates via Sacco's mobile and electronic services

ii. Indirectly:

- a) From other people who think that the data subject may be interested in collaborating in our work.
- b) From the public domain when the data subject has deliberately made the data public.
- c) From third parties such as previous or current employers to verify details about job applicants.
- d) From external sources such as publications and external reviewers or advisors.
- e) From another source when the guardian appointed has consented to the collection in cases where the data subject has incapacity.
- f) Where collection of data from another source is necessary:
 - for the prevention, detection, investigation, prosecution and punishment of crime.
 - for the enforcement of a law which imposes a pecuniary penalty; or
 - For the protection of the interests of the data subject or another person.

23 Forms of personal information collected

The Sacco only collects personal information that is genuinely needed for its operations. This may include:

- Contact details such as name address, email address and phone numbers
- Biometric data such as thumb prints
- Nationality
- National ID and Passport information
- Date of birth
- Gender
- Information about race and ethnicity
- Qualifications
- Bank account details
- Medical information
- Benefits received
- Employment details
- Photographs and video recordings

-
- Tax and residency status for statutory requirements
 - References from previous employers or educational institutions
 - Contact details for family members and next of kin
 - Details of criminal convictions
 - Next of kin
 - Certificate of good conduct
 - CRB certificate
 - Wealth declaration

2.4 Personal Data Protection Principles

In processing personal data, Mariakani Mabati Sacco shall be guided by the principles of data protection as captured in the Data Protection Act, and requires the Sacco to ensure that personal data is:

- a) Processed in accordance with the right to privacy of the data subject;
- b) Processed lawfully, fairly and in a transparent manner in relation to any data subject;
- c) Collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes;
- d) Adequate, relevant, limited to what is necessary in relation to the purposes for which it is processed;
- e) Collected only where a valid explanation is provided whenever information relating to family or private affairs is required;
- f) Accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data is erased or rectified without delay;
- g) Kept in a form which identifies the data subjects for no longer than is necessary for the purposes which it was collected; and
- h) Not transferred outside the Sacco and the country, unless there is proof of adequate data protection safeguards or consent from the data subject.

In complying with the stated data protection principles, Mariakani Mabati Sacco will observe the following:

2.4.1 Fairness and lawfulness

When processing personal data, the individual rights of the data subjects must be protected. Personal data must be collected and processed in a legal and fair manner.

2.4.2 Restriction to a specific purpose

Personal data can be processed only for the purpose that was defined before the data was collected. Subsequent changes to the purpose are only possible to a limited extent and require substantiation.

2.4.3 Transparency

The data subject must be informed of how his/her data is being handled. In general, personal data must be collected directly from the individual concerned. When the data is collected, the data subject must either be aware of, or informed of:

- a) The identity of the Data Controller
- b) The purpose of data processing
- c) Third parties or categories of third parties to whom the data might be transmitted, if any.

2.4.4 Data reduction and data economy

Before processing personal data, the Sacco will determine whether, and to what extent the processing of personal data is necessary to achieve the purpose for which it is undertaken. Where the purpose allows and where the expense involved is in proportion with the goal being pursued, anonymized or statistical data must be used. Personal data may not be collected in advance and stored for potential future purposes unless required or permitted by national law.

2.4.5 Deletion

Personal data that is no longer needed after the expiration of legal or business process- related periods must be deleted. There may be an indication of interests that merit protection or historical significance of this data in individual cases. If so, the data must remain on file until the interests that merit protection have been clarified legally, or the Sacco has evaluated the data to determine whether it must be retained for historical purposes.

2.4.6 Factual accuracy; up-to-date data

Personal data on file must be correct, complete, and – if necessary – kept up to date. Suitable steps must be taken to ensure that inaccurate or incomplete data are deleted, corrected, supplemented or updated.

2.4.7 Confidentiality and data security

Personal data is subject to data secrecy. It must be treated as confidential on a personal level and secured with suitable organizational and technical measures to prevent unauthorized access, illegal processing or distribution, as well as accidental loss, modification or destruction.

2.5 Rights of the Data Subject

Every data subject has the following rights:

- a) To be informed of the use to which their personal data is to be put;
- b) To access their personal data in custody of data controller or data processor;
- c) To object to the processing of all or part of their personal data. This does not apply if a legal provision requires the data to be processed;
- d) To correction of false or misleading data; and
- e) To deletion of false or misleading data about them.

A right conferred on a data subject may be exercised:

- a) by a person who has parental authority or by a guardian if the data subject is a minor;
- b) by a person duly authorized to act as a guardian or administrator in a case where the data subject has a mental or other disability; or
- c) by a person duly authorized by the data subject.

2.6 Data Subject Consent

A data subject may prior to the processing of their personal data give consent either orally or in writing, and may include a handwritten signature, an oral statement, or use of an electronic or other medium to signify agreement.

The Sacco shall seek consent from data subjects through various means. These include the data subjects willingly:

- i. Appending their signature of acceptance of terms and conditions of engagement on physical consent form.
- ii. Ticking an opt-in box on paper or electronically.
- iii. Clicking an opt-in button or link online.
- iv. Responding to an email requesting consent.
- v. Volunteering optional information for a specific purpose.
- vi. Selecting from equally prominent Yes/No options.

In obtaining consent from a data subject, the Sacco shall ensure that the data subject:

- a) has capacity to understand and communicate their consent;
- b) is informed of the nature of processing in simple and clear language that is understandable;
- c) Is informed whether data is being transferred to third party or implementing partners, or whether data is being collected by a third party on behalf of Mariakani Mabati Sacco.
- d) Is informed of their duty to keep Mariakani Mabati Sacco informed of changes to their personal data and status.
- e) Is informed of right to access to their personal data, or correction or deletion of it.
- f) Is informed of procedure to lodge a complaint in case of suspected breach.
- g) Is informed of the importance of providing accurate and complete information.
- h) Voluntarily gives consent and that the consent is specific.

Example



If you don't want us to share your response with ABC company please tick here ☐



If you would like us to share your response with ABC company please tick here ☐

2.7 Confidentiality of Data Processing

Personal data is subject to data secrecy. Any unauthorized collection, processing, or use of such data by employees is prohibited. Any data processing undertaken by an employee that he/she has not been authorized to carry out as part of his/her legitimate duties is unauthorized. The “need to know” principle applies. Employees may have access to personal information only as is appropriate for the type and scope of the task in question. This requires a careful breakdown and separation, as well as implementation, of roles and responsibilities.

Employees are forbidden to use personal data for private or commercial purposes, to disclose it to unauthorized persons, or to make it available in any other way. Supervisors must inform their employees at the start of the employment relationship about the obligation to protect data secrecy. The staff shall therefore sign an oath of secrecy at the time of engagement by the Sacco. This obligation shall remain in force even after employment has ended.

2.8 Data Processing Security

Personal data must be safeguarded from unauthorized access and unlawful processing or disclosure, as well as accidental loss, modification or destruction. This applies regardless of whether data is processed electronically or in paper form. Before the introduction of new methods of data processing, particularly new IT systems, technical and organizational measures to protect personal data must be defined and implemented. These measures must be based on the state of the art, the risks of processing, and the need to protect the data.

In particular, the responsible staff can consult with the Sacco’s CEO. The technical and organizational measures for protecting personal data are part of the Sacco’s data security management and will be adjusted continuously to the technical developments and organizational changes.

2.9 Duration for holding personal information

The Sacco will hold personal information for as long as is necessary and will therefore not retain personal information if it is no longer required. In some circumstances, the Sacco may legally be required to retain data subject's personal information, for example for finance, employment or audit purposes.

2.10 Data Breach and Notification

Data Breach includes but not limited to the following

- a) Unauthorized disclosure of Personal Data belonging to staff members, board of directors or customer personal data;
- b) Loss or theft of confidential or sensitive data;
- c) Loss or theft of equipment on which Personal Data is stored (e.g. loss of laptop, USB stick, iPad/tablet device, or paper record);
- d) Unauthorized use of, access to or modification of IT, data or information Systems (e.g. via a hacking attack); and
- e) Attempts (failed or successful) to gain unauthorized access to IT, data or Information systems.

If any member of Staff, or other person learns of a suspected or actual Personal Data Breach, it must be reported to immediately or within 12hours to the senior management or the data protection officer.

2.10.1 Notification to the ODPC

The Mariakani Mabati Sacco shall promptly notify the Office of the Data Protection Commissioner (ODPC) upon becoming aware of personal data breach involving data subject within its records and properly record the breach. The Sacco shall also undertake to inform the data subject within reasonable time of the breach on their personal data and explain mitigating measure taken to safeguard the data and address potential adverse effects of the breach. **DATA RESPONSIBILITIES**

3.1 Organizational responsibilities

3.1.1 Policies and Procedures

Mariakani Mabati Sacco being the Data Controller, is responsible for establishing policies and procedures in order to comply with the relevant and applicable data protection laws.

3.1.2 Data Protection Impact Assessment (Privacy Assessment)

-
- a) The Sacco being a Data Controller shall undertake to carry out a Privacy Impact assessment to identify and minimize risks involved in projects, processes and activities involving directly or indirectly processing of personal data.
 - b) The DPIA will be required for processing where there is a likelihood of high risk to individuals and their personal data and where new technologies are involved.
 - c) The Data Protection Officer shall undertake the privacy assessment in assistance with relevant department and sign off the reports.

3.2 Data Protection Officer Responsibilities

The Data Protection Officer is responsible for:

- I. Advising the Sacco and its staff of its obligations under relevant data protection laws and regulations.
- II. Monitoring compliance with this Policy and other relevant data protection laws, and monitoring training activities that relate to data protection compliance.
- III. Providing advice where requested on data protection impact assessments.
- IV. Having due regard to the risk associated with processing operations, considering the nature, scope, context and purposes of processing.
- V. Maintaining data inventories of all personal information within Sacco and those provided by external data controllers and processors, including data transfer agreements, specific instances of data sharing by third parties, data protection impact assessments, data breach notifications and complaints by data subjects.
- VI. Conducting awareness training on staff members on data privacy and security.

3.3 Staff responsibilities

Staff members who process personal data about Sacco members, current and previous staff, applicants, interns, or any other individual must comply with the requirements of this policy.

Staff members must ensure that:

- a) All personal data is kept securely;
- b) No personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorized third party;
- c) Personal data is kept in accordance with the Sacco's retention schedule.

-
- d) Any queries regarding data protection, including subject access requests and complaints, are promptly directed to the Data Protection Officer;
 - e) Any data protection breaches are swiftly brought to the attention of the Human Resource and Administration team for staff data and the Data Protection Officer, and that they support the team in resolving breaches;
 - f) Where there is uncertainty around a data protection matter advice is sought from the Human Resource Manager for staff data or the Data Protection Officer.

Where members of staff are responsible for supervising external service providers doing work which involves the processing of personal information, they must ensure that such external persons are aware of the Sacco's organizational Data Protection principles.

Staff who is unsure about who are the authorized third parties to whom they can legitimately disclose personal data should seek advice from the CEO through their line managers.

3.4 Third-Party Data Processors

Where external companies are used to process personal data on behalf of the Sacco, responsibility for the security and appropriate use of that data remains with the Sacco.

Where a third-party data processor is used:

- a) a data processor must be chosen which provides sufficient guarantees about its security measures to protect the processing of personal data;
- b) reasonable steps must be taken that such security measures are in place;
- c) a written contract establishing what personal data will be processed and for what purpose must be set out;
- d) A data processing agreement must be signed by both parties.
- e) Mariakani Mabati Sacco being the data owner will be ultimately responsible for the data being processed by the third party vendors.

In the event of termination of partnership, all personal data collected for or on behalf of the Sacco by the third party shall be returned to Mariakani Mabati Sacco as stipulated in the agreement except where exceptions were provided for in the signed service level agreements (SLA's) or where there's legitimate reasons to do so such as consent of data subjects.

3.5 Contractors and Temporary Staff

The Sacco is responsible for the use made of personal data by anyone working on its behalf. The Sacco shall ensure that contractors and staff working on short-term engagement are appropriately vetted for the data they will be processing. In addition, managers should ensure that:

- a) Any personal data collected or processed in the course of work undertaken for the Sacco is kept securely and confidentially.
- b) All personal data is returned to the Sacco upon completion of the work, including any copies that may have been made. Alternatively, that the data is securely destroyed, and the Sacco receives written notification in this regard from the contractor or short-term member of staff;
- c) The Sacco receives prior notification of any disclosure of personal data to any other organization or any person who is not a direct employee of the contractor;
- d) Any personal data made available by the Sacco, or collected in the course of the work, is neither stored nor processed outside Kenya unless written consent to do so has been received from the Sacco;
- e) All practical and reasonable steps are taken to ensure that contractors, short term or voluntary staff do not have access to any personal data beyond what is essential for the work to be carried out properly.

3.0 COMPLIANCE

- 7.1 All officials, staff and stakeholders of the Sacco shall comply with the provisions of this Policy.
- 7.2 To ensure compliance, officials, staff of the Sacco shall sign an oath of confidentiality committing to treat accessed personal information securely and in confidentiality. Stakeholders' contracts shall have a clause on confidentiality on accessed personal information. The oath shall be binding during and after exit from service of the Sacco.
- 7.3 Staff not complying with this Policy shall face disciplinary action in line with the Human Resource Policy.

-
- 7.4 Sacco officials not complying shall face disciplinary action in line with the Sacco Bylaws, Board Charter and relevant laws and regulations.
- 7.5 External service providers not complying with the provisions of this policy will be handled in accordance with provisions of contracts signed.

POLICY REVISION

This Policy shall be reviewed periodically and may be amended as conditions warrant. Amendments to this Policy may be recommended by staff through the CEO or by individual Directors as necessary and submitted to the Board, provided the changes in no way affect the substance or intent of this Policy. Amendments and updates to this policy shall become effective only when adopted by a BOD resolution.

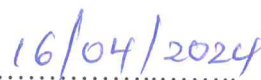
ADOPTION OF POLICY

This document may be cited as the Data Protection Policy for Mariakani Mabati Sacco Society Limited and has been discussed and adopted for implementation this day of 2023.

Mr. Mathew Odanga
Chairperson



Signature

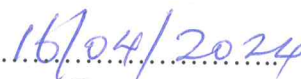


Date

Mr. Nicodemus Sanga
Vice-Chairperson



Signature

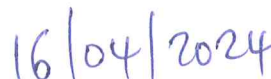


Date

Mr. Vincent Onyango
Treasurer



Signature



Date

Mr. Isaac Mutisya
Hon. Secretary



Signature



Date

Mr. Crispus Kidundu



Signature



Date

**Public Relations
Officer**

APPENDIX I: OATH OF CONFIDENTIALITY/SECREC

I, the undersigned, DANIEL SIAI,

(FULL NAMES)

being an employee of Mariakani Mabati Sacco Society Ltd, hereby declare:

That I will treat securely and observe strict confidentiality in respect to all personal data relating to Sacco officials, staff, members/customers and stakeholders and will not reveal any of the matters which may come to my knowledge in the discharge of my duties during and after engagement by the Sacco, except where and when required to do so by the Board of Directors, the Supervisory Committee, The Chief Executive Officer, or other person duly authorized in writing by the Society or by a court of law, or by any other person to whom such matters relate provided such person is entitled to be informed in respect thereof.

Signature: [Signature] Department/Branch: ACCOUNTS

Date: 16/04/2024

Witnessed by: MARRION DAMA

(FULL NAMES)

Signature of Witness: [Signature] Date 16/04/2024

APPENDIX II: THIRD PARTIES/PARTNERS' NON-DISCLOSURE AGREEMENT

We/I, the undersigned,

CRISPUS MNYOGHA KIDUNDO

(FULL NAMES)

being service provider(s) of Mariakani Mabati Sacco Society Ltd, hereby declare that:

We/I undertake that during the operation of, and after the expiration, termination or cancellation of this appointment, for any reason, we/I will keep confidential any proprietary or confidential data/information relating to the Sacco or its services or members/customers or stakeholders.

Any studies, reports or other materials, graphics, software or otherwise received or prepared by us/me from/for the Sacco under this Agreement shall belong to and remain the property of the Sacco. We/I shall not use such property for any other purpose unless prior express consent is given by the Sacco.

In the event of a breach and Sacco data has been exposed you will take necessary action to mitigate the risk and inform the Sacco within 48hours of the breach being known.

Authorised signatory:

Name: CRISPUS MNYOGHA KIDUNDO Designation: PUBLIC RELATIONS

Signature: 

OFFICER

Date: 16/4/2024

Witnessed by:

Name: Daniel Sitati

Signature: 

Date: 16/04/2024