Data Protection and Privacy Policy

Original issue date	December 2022
Approver	Board of Directors
Owner	Head of Risk and Compliance
Reviewed date	March 2024
Next review date	March 2027
Version	2

Table of content

1. Introduction

LOLC UNGUKA FINANCE Plc gather and use certain information about individuals. These include information about customers, suppliers, business contacts, employees, and other people the organisation has a relationship with or may need to contact. This policy describes how these personal data must be collected, handled, and stored to meet the company's data protection standards — and to comply with the laws and regulations.

This data protection policy ensures LOLC UNGUKA FINANCE Plc:

- Complies with data protection law, regulations and follow good practice.
- Protects the rights of staff, customers, and partners.
- Is open about how it stores and processes individuals' data.
- Protects itself from the risks of a data breach.

Protecting the confidentiality and integrity of personal data, it is a critical responsibility that LOLC UNGUKA FINANCE Plc always take data protection with high importance. This policy is therefore intended to apply to the personal data that LOLC UNGUKA FINANCE Plc collects and processes about its employees, customers, suppliers and other third parties.

2. Definitions

For ease of understanding this section defines the various terms used in the document to avoid any misunderstandings among the members of the organization.

- **Personal data:** Any information relating to a natural person who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, an online identifier or to one or more factors specific to the physical, genetic, mental, economic, cultural, or social identity of that natural person.
- **Sensitive personal data:** Information revealing a person's race, health status, criminal records, medical records, social origin, religious or philosophical beliefs, political opinion, genetic or biometric information, sexual life, or family details.
- **Data controller:** means a person who (either alone or. jointly or in common with other persons) determines the purposes for which and the way any personal data are or are to be processed. LOLC UNGUKA FINANCE Plc determines the purposes and means of processing personal data, such as customer information, transaction records, and financial information. As a data controller, LOLC UNGUKA FINANCE Plc is also responsible for complying with data protection laws, ensuring that personal data is processed lawfully, fairly and transparently, and protecting the rights of the data subjects.
- **Data processor:** The data processor processes personal data only on behalf of the controller. The data processor is usually a third-party external to the company. LOLC UNGUKA FINANCE Plc may engage with third-party data processors to perform certain processing activities on their behalf. However, the data processor must provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing meets the requirements of data protection and privacy law.
- **Data subject:** A natural person about whom a controller holds personal data and who can be identified, directly or indirectly, by reference to that personal data.

- **Consent of the data subject:** Freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by an oral, written, or electronic statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
- **Processing of personal data:** This refers to activities such as the collection, storage, use, transfer, and disclosure of personal data. All activities involving personal data, from the planning of processing to the erasure of personal data, constitute processing of personal data.
- **Privacy:** fundamental right of a person to decide who can access his or her personal data, when, where, why, and how his or her personal data can be accessed.

3. Scope

This policy applies to all personal data that the company process regardless of the media on which that data is stored (Whether physical or digital). The policy applies to:

- The head office of LOLC UNGUKA FINANCE Plc
- All branches, all outlets of LOLC UNGUKA FINANCE Plc
- All clients, staff, and volunteers of LOLC UNGUKA FINANCE Plc
- All contractors, suppliers and other people working on behalf of LOLC UNGUKA FINANCE Plc

It applies to all data that the company holds relating to identifiable individuals. These include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Identity card and passport
- Date and place of birth
- Identification of relatives
- Fingerprints
- Medical reports

Anyone who works for LOLC UNGUKA FINANCE Plc must read, understand, and comply with this document when processing personal data. Any breach of the rules contained in this document will result in disciplinary action.

4. Personal Data Processing principles

LOLC UNGUKA FINANCE Plc Management, Boards and employees process personal data with all due care so that only necessary and accurate personal data are processed by authorized employees, in a legitimate, secure, and transparent manner, and for specific and limited purposes. To this end, the Bank is committed to the following principles regarding the processing of personal data:

a. Lawfulness

LOLC UNGUKA FINANCE Plc is committed to ensuring that all processing of personal data is carried out in accordance with the law and that all necessary measures are taken to protect

the rights and freedoms of data subjects. We process personal data if (at least) one of the following lawful processing grounds applies:

- Where the processing is based on consent.
- If the processing is necessary for the performance of a contract,
- If the processing is necessary for compliance with a legal obligation.
- If the processing is necessary for safeguard of a vital interest
- If the processing is necessary for the performance of a task in the public interest or the exercise of official authority, and/or
- If the processing is necessary for the purposes of the legitimate interests pursued by LOLC UNGUKA FINANCE Plc or a third party.

b. Honesty and transparency

The processing of personal data is carried out with the utmost transparency towards the data subjects to enable them to understand why and how their personal data is used LOLC UNGUKA FINANCE Plc as well as their rights in terms of data protection. This transparency is a prerequisite for fair processing as it allows data subjects to maintain control over their personal data.

c. Purpose limitation

The Bank is committed to collect personal data for specific, explicit, and legitimate purposes. Any re-use of personal data for purposes other than those originally intended is not allowed unless the data subjects have been informed of that re-use and have given their consent.

d. Data minimization and accuracy

LOLC UNGUKA FINANCE Plc is committed to ensure that personal data processed is adequate, relevant, and limited to what is necessary. In accordance with the relevant internal policies and procedures, all reasonable steps to maintain the accuracy of personal data shall be taken. In view of the purposes for which they are processed, personal data that is incorrect will be rectified or deleted without delay.

e. Limitation of retention

LOLC UNGUKA FINANCE Plc is committed to not retain personal data (including data on documents) for longer than necessary. LOLC UNGUKA FINANCE Plc's Management, and employees ensure that a data retention period is maintained based on the data retention policy. At the end of the retention periods, personal data will be destroyed, deleted, or anonymized in accordance with applicable internal policies and procedures.

f. Integrity, security, and confidentiality

LOLC UNGUKA FINANCE Plc is committed to process personal data in such a way as to ensure appropriate security. In particular, the Bank takes care to prevent unauthorized or unlawful processing and loss, destruction, or damage of accidental origin. In this respect, LOLC UNGUKA FINANCE Plc’s Management Boards and employees update their knowledge of internal policies and procedures relating to information security. LOLC UNGUKA FINANCE Plc is required to report personal data breaches in a timely manner in accordance with the regulations.

5. Data Subject consent

Before processing personal data of a data subject, LOLC UNGUKA FINANCE Plc is required to get consent from the data subject using a data subject consent form. In case LOLC UNGUKA FINANCE Plc or its third-party processor know that the personal data being processed belong to a child under the age of sixteen (16) years, a consent must be obtained from a holder of parental responsibility over the child in accordance with relevant laws. Subject to the provisions of other laws, the consent obtained on behalf of the child is acceptable only if it is given in the interest of the child. This is done using by completing a parental consent form.

6. Information to be provided during personal data collection

LOLC UNGUKA FINANCE Plc should collect personal data for a lawful purpose connected to the activities of the bank and when the data is necessary for that purpose.

When collecting personal data, LOLC UNGUKA FINANCE Plc should inform the data subject of the following:

- Its identity and contact details.
- The purpose for which the personal data are collected.
- Recipients of such personal data.
- Whether the data subject has the right to provide personal data voluntarily or mandatorily.
- The existence of the right to withdraw consent at any time and that such withdrawal does not affect the lawfulness of the processing of personal data based on consent before its withdrawal.
- The existence of the right to request from LOLC UNGUKA FINANCE Plc access and rectification, restriction, or erasure of personal data concerning the data subject to the processing of the data.
- The existence of automated decision-making, including profiling, and information about the logic involved, as well as the significance and the envisaged consequences of such processing personal data for the data subject.
- The period for which personal data will be stored.
- The right to appeal to the supervisory authorities.
- Where applicable, that LOLC UNGUKA FINANCE Plc can transfer personal data outside Rwanda, and it assures of the security of the data and must comply to the requirements stipulated in Rwandan law relating to the protection of personal data and privacy

7. Recipients of Personal data

LOLC UNGUKA FINANCE Plc has several departments that collect, process, and store personal data, including Human Resources, Risk and Compliance, Business, and IT. These departments play a critical role in ensuring personal data privacy by implementing appropriate technical and organizational measures to safeguard personal data.

To ensure compliance with data protection laws and regulations, LOLC UNGUKA FINANCE Plc shall put in place controls, such as:

- Regular audits and assessments to monitor compliance with data protection regulations and identify areas for improvement.
- Appointment of a data protection officer to oversee data protection activities and ensure compliance with relevant laws and regulations.
- Implementation of data retention and deletion policies to ensure that personal data is not stored for longer than necessary.
- Conducting regular vulnerability assessments and penetration testing to identify and address any security vulnerabilities.
- Developing and implementing incident response plans to handle data breaches and other security incidents.
- Using access controls, such as passwords and authentication protocols, to restrict access to personal data to authorized personnel only.

To carry out the processing activities in accordance with the legal bases set out by each Data controller, LOLC UNGUKA FINANCE Plc may send some personal data to internal and external recipients:

- Organizational parts of LOLC UNGUKA FINANCE Plc (i.e., any department of LOLC UNGUKA FINANCE Plc that may help achieve the purpose pursued by the Data controller).
- Public authorities (e.g., public prosecutor, collector general of taxes, national social security, etc.).
- External organizations (e.g., Data processor, brokers and insurers, notaries, lawyers, etc).
- Internal and/or external auditors.

8. Responsibilities

Everyone who works for or with LOLC UNGUKA FINANCE Plc has some responsibility for ensuring data is collected, stored, and handled appropriately. Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles. However, these people have key areas of responsibility:

- The **Board of Directors** is ultimately responsible for ensuring that LOLC UNGUKA FINANCE Plc meets its legal obligations. In addition to its overarching governance responsibilities, the Board of Directors is responsible for the following specific data protection responsibilities:
  - Approving and overseeing the implementation of data protection policies, procedures, and controls.
  - Establishing and maintaining a data protection culture throughout the organization, emphasizing the importance of data protection to all employees and stakeholders.
  - Approving and monitoring the budget for data protection measures and resources, such as training, software, and hardware.
  - Reviewing and monitoring data protection risk assessments, including the identification of potential threats and vulnerabilities, and ensuring that appropriate measures are in place to mitigate them.
  - Ensuring that the Data Protection Officer and other relevant departments have sufficient resources and authority to carry out their responsibilities effectively.

- The Senior Management has the responsibility of implementing the data protection policies and ensuring that they are followed throughout the organization. The specific responsibilities of senior management can include:

  - Ensuring that data protection policies and procedures are implemented and followed throughout the organization.
  - Providing the necessary resources for data protection measures, such as training and equipment.
  - Appointing the Data Protection Officer and other relevant personnel responsible for data protection and ensuring that they have the necessary resources and authority to carry out their responsibilities effectively.
  - Reporting to the Board of Directors on the implementation of data protection policies and any related issues, risks, and incidents.
  - Conducting regular reviews of data protection policies and procedures and updating them as necessary.

- The Information Security and Data Protection Manager, is responsible for:

  - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
  - Performing regular checks and scans to ensure security hardware and software is functioning properly.
  - Evaluating any third-party services, the company is considering using to store or process data. For instance, cloud computing services.
  - Keeping the Management updated about data protection responsibilities, risks, and issues.
  - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
  - Arranging data protection training and advice for the people covered by this policy.
  - Handling data protection questions from staff and anyone else covered by this policy.
  - Dealing with requests from individuals to see the data LOLC UNGUKA FINANCE Plc holds about them (also called 'subject access requests').
  - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

- The Risk and Compliance Department is responsible for:
  - Coordinate the risk assessment associated with the processing of personal data.
  - Developing and implementing risk management strategies to minimize the risk of data breaches and other related risks.
  - Conducting an assessment to review the compliance status with data protection laws and regulations and provide recommendations and follow up on them.
  - Developing and delivering data protection training to employees to ensure they understand their responsibilities and are compliant with data protection policies and procedures.

- Preparing reports to the board of directors and management on data protection risks and compliance issues.

- The Audit Department is responsible for:
  - Performing regular audits and assessments of data protection policies, procedures, and controls to ensure they are effective and comply with relevant legal requirements.
  - Identifying and reporting on any gaps or weaknesses in data protection controls and making recommendations for improvements.
  - Providing assurance to the Board of Directors and senior management that data protection risks are being effectively managed and mitigated.
  - Reviewing and evaluating the effectiveness of data protection training and awareness programs to ensure they are meeting their objectives.
  - Conducting investigations in the event of data breaches or other incidents involving personal data and reporting on the findings to the appropriate parties.
    Ensuring that the Data Protection Officer and other relevant departments are providing accurate and complete reporting on data protection incidents and risks.

9. General Staff guidelines

The following are general staff guidelines to follow when dealing with data in the organization:

- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
- LOLC UNGUKA FINANCE Plc should provide training to all employees to help them understand their responsibilities when handling personal data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- Strong passwords must be used, and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within the company or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection.

10. Record keeping

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager or data controller. When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion, and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (like flash drives or external hard disks), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers and should only be uploaded to a cloud computing service.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested on a monthly basis in line with the bank's standard backup procedures.
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by approved security software and a firewall.

Personal data is of no value to LOLC UNGUKA FINANCE Plc unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption, or theft. With that in mind the following rules must be observed:

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally. It should never be sent by through unencrypted communication channels.
- Data must be encrypted before being transferred electronically.
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

The law requires LOLC UNGUKA FINANCE Plc to take reasonable steps to ensure data is kept accurate and up to date. The more important it is that the personal data is accurate, the greater the effort LOLC UNGUKA FINANCE Plc should put into ensuring its accuracy. It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.
- LOLC UNGUKA FINANCE Plc will make it easy for data subjects to update the information LOLC UNGUKA FINANCE Plc holds about them.
- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it may be removed from the database subject to the approval of the Management.

LOLC UNGUKA FINANCE Plc shall keep records on the identification data obtained through or presented during the customer (or any other stakeholders) transaction process within a period of at least 10 years after the end of business relationship.

LOLC UNGUKA FINANCE Plc shall maintain in accordance with the data protection laws a record of all personal data processing activities under its responsibility. These records indicate:

- the name and contact details of the data controller and, where applicable, the data processor, the controller's representative or the data protection officer.
- the purposes of the processing of personal data;
- a description of the categories of data subjects and of the categories of personal data;
- a full list of the recipients to whom personal data have been or will be disclosed, including those based in other countries;
- a description of transfers of personal data to any country outside Rwanda;
- where possible, the envisaged data retention periods for the different categories of personal data.

LOLC UNGUKA FINANCE Plc shall also submit the records of personal data processing activities to the supervisory authority upon request.

11. Personal Data Breaches

Notification to the supervisory authority: In the case of a personal data breach, LOLC UNGUKA FINANCE Plc will without undue delay and, where feasible, not later than 48 hours after having become aware of it, notify the personal data breach to the supervisory authority (National Cybersecurity Authority) unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 48 hours, it shall be accompanied by reasons for the delay.

In a period of not later than 72 hours, LOLC UNGUKA FINANCE Plc will draw up a report on personal data breach and submits it to the supervisory authority with all facts available.

The report shall describe at least:

- Describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned.
- Communicate the name and contact details of the data protection officer or other contact point where more information can be obtained.
- Describe the likely consequences of the personal data breach.
- Describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Notification to the data subject: In case the personal data breach is likely to result in a high risk to the rights and freedoms of the data subject, LOLC UNGUKA FINANCE Plc will communicate the personal data breach to the data subject in writing or electronically after having become aware of it.

12. Data subject rights

All individuals who are the subject of personal data held by LOLC UNGUKA FINANCE Plc are entitled to the following rights:

- **Right to personal data:** Without prejudice to other relevant Laws, the data subject may, in writing or electronically, request from LOLC UNGUKA FINANCE Plc the following:
  - to provide him or her with the information relating to the purposes of the processing of personal data.
  - to provide him or her with a copy of personal data.
  - to provide him or her with a description of personal data that the bank holds, including data on the contact details of a third party or the categories of third parties who have or had access to personal data.
  - to inform him or her of the source of the personal data in case his or her personal data has not been obtained from the data subject.
  - to inform him or her in case his or her personal data has been transferred to a third country or to an international organization.
- **Right to personal data portability:** The data subject has the right to request LOLC UNGUKA FINANCE Plc in writing or electronically to resend the personal data concerning him or her as it was provided, in a structured and readable format. The data subject also has the right to request LOLC UNGUKA FINANCE Plc in writing or electronically to have his or her personal data transmitted to another data controller, where technically feasible, without hindrance.
- **Right not to be subject to a decision based on automated data processing:** The data subject has the right not to be subject to a decision based solely on automated personal data processing, including profiling, which may produce legal consequences or significant consequences to him or her.
- **Right to restriction of processing:** The data subject or the supervisory authority has the right to restrict the data controller from processing personal data for a given period if:
  - The accuracy of personal data is contested by the data subject, pending the verification of their accuracy.
  - The processing is unlawful, and the data subject requests the erasure of the personal data or the restriction of the use of some of them.
  - The data subject has objected to the processing of personal data pending the verification whether the legitimate grounds of the controller override those of the data subject.
- **Right to erasure of personal data:** the data subject has the right to request the data controller in writing or electronically for erasure of his or her personal data where:
  - Personal data are no longer necessary in relation to the purposes for which they were collected or processed.
  - The data subject withdraws consent on which the personal data processing is based and where there is no other legal ground for the processing.
  - The data subject objects to the processing of personal data and there are no overriding legitimate grounds for the processing.
  - Personal data have been unlawfully processed.
- **Right to rectification:** The data subject has the right to request the data controller the rectification of his or her personal data. The data subject has the right to have

incomplete personal data completed, where necessary. LOLC UNGUKA FINANCE Plc, within thirty (30) days from the date of receipt of the request, must inform the data subject in writing or electronically of the rectification of his or her personal data.

- **Right to designate an heir to personal data:** The personal data of the data subject are not subject to succession. However, where the data subject had left a will, the data subject provides his or her heir with full or restricted rights relating to the processing of personal data kept by the data controller or the data processor, if such personal data still need to be used.
- **Right to representation:** The right of the data subject to representation is exercised where:
  - the data subject is under sixteen (16) years of age, in which case he or she is represented by a person who has parental authority over him or her or who was appointed as his or her guardian.
  - the data subject has a physical impairment and is unable to represent himself or herself, in which case he or she is represented by his or her parent, adopter, a center or an association that caters for him or her guardian appointed by a court.
  - the data subject has a medically determinable mental impairment and is unable to represent himself or herself, in which case he or she is represented by his or her parent, adopter, a center or an association that caters for him or her or the guardian appointed by a court.
  - there is any other reason, in which case he or she is represented by another person authorized in writing by the data subject in accordance with relevant law.
- **Right to withdraw consent:** The data subject has the right to withdraw his or her consent at any time. The withdrawal of consent does not affect the lawfulness of processing of personal data based on consent before its withdrawal. The withdrawal of consent by the data subject is as easy as expressing it. The withdrawal of consent by the data subject takes effect as of the date on which the data subject applied for it.

13. Sharing personal data

LOLC UNGUKA FINANCE Plc generally only share personal data with its third parties, such as third-party service providers under the following circumstances:

- The third party needs to hold the data to provide the contracted services.
- The privacy notice given to the data subject has made it clear that their data will be given to third parties for express purpose.
- The third party has agreed to comply with the necessary data security standards and procedures.
- There exists a DPA (Data Protection Act) compliant contract between both parties.
- The transfer of data complies with cross-border transfer restrictions.

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, LOLC UNGUKA FINANCE Plc will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

14. Personal data processed by a data processor

LOLC UNGUKA FINANCE Plc is also committed to ensure that all data processors are authorized in accordance with the requirements set forth in Article 4 of the law relating to the protection of personal data and privacy and that all processing activities are carried out in compliance with the written contract and applicable data protection regulations.

Any processing of personal data by a third-party data processor will be subject to a written contract between the bank and the data processor, which outlines the terms and conditions of the processing activities, the nature and purpose of the processing, and the obligations and responsibilities of the data processor.

As the data controller, LOLC UNGUKA FINANCE Plc will authorize the data processor to process personal data only if the data processor can provide sufficient guarantees that appropriate technical and organizational measures will be implemented to ensure that the processing meets the requirements of the law. These measures may include, but are not limited to, ensuring the confidentiality and security of the personal data, carrying out data protection impact assessments, and implementing measures to ensure the rights of data subjects are protected.

15. Training and awareness on Data Protection and Privacy

LOLC UNGUKA FINANCE Plc recognizes that data protection and privacy are crucial components of its operations, and that all personnel must be equipped with the necessary knowledge and skills to ensure that personal data is processed in a secure and compliant manner. To achieve this, the following measures are put in place:

- **Development of Training and Awareness Program:** The Data Protection Officer is responsible for developing and maintaining a comprehensive data protection and privacy training and awareness program for all stakeholders. The program will cover topics such as the principles of data protection and privacy, the data protection and privacy law of Rwanda, and the bank's policies and procedures for handling personal data.

- **Allocation of Resources for Specialized Training:** LOLC UNGUKA FINANCE Plc management shall put in place adequate resources to ensure that relevant personnel, such as the Data Protection Officer (DPO), are nominated and sponsored for specialized and specific trainings in cybersecurity, data protection and privacy. This will help to ensure that the DPO and other relevant personnel have the necessary knowledge and skills to implement effective data protection and privacy measures.

- **Awareness on Basic Principles of Data Protection and Privacy:** All employees, contractors, and third-party personnel shall receive regular awareness on the basic principles of data protection and privacy, as well as Rwanda's data protection and

privacy law. This is to ensure that all personnel understand the importance of protecting personal data, and the consequences of non-compliance with data protection and privacy regulations.

16. Measures for personal data access

At LOLC UNGUKA FINANCE Plc, protecting personal data is of critical priority. To ensure proper access to personal data collected by LOLC UNGUKA FINANCE Plc, the following measures have been implemented:

- **Privileged Access Management (PAM):** We use a PAM solution to control elevated access and permissions for users, accounts, processes, and systems across our IT environment. This helps condense our attack surface and prevent, or at least mitigate, the damage arising from external attacks or insider malfeasance or negligence.

- **Network Access Control (NAC):** We use NAC solutions to ensure that non-employees have access privileges to the network that are separate from those of employees, accounting for contractors, visitors, or partners.

- **Controlled Admittance:** To prevent unauthorized users from accessing data processing systems, we use the following measures for user identification and authentication:
  - Systems are protected by employee usernames and passwords.
  - Passwords are protected using policies and technologies and are required to change periodically.
  - Users are identified through an Active Directory.
  - Users only have access to applications/data based on their roles and are only able to view their own information.
  - Idle client systems are locked automatically after a defined time and can be unlocked by the user using their password.
  - Network security is managed by our internal IT team, and physical and logical access to data centers are restricted to authorized employees responsible for the job.

- **Disclosure Control**: When transmitting critical and sensitive data, we use secure encrypted channels of communication like SSL, Secured VPN, SFTP, and access applications using HTTPS.

- **Separation Control:** Data collected for different purposes are processed separately. All environments, documents, and other data are shared with the members of that project/product.

- **Access Control:** To control physical access to LOLC UNGUKA FINANCE Plc's premises and identify authorized people, we have implemented the following measures:
  - Entrance to the building is only possible with fingerprints and keycards provided to employees.
  - Certain locations are physically locked, and access is restricted to authorized employees only (e.g., Server Room).

Data Control: In order to monitor data access, alterations, disclosures, or transfers, we implemented a data leakage prevention solution to ensure that all activities and processes are logged and tracked.

17. Information Security Safeguards

LOLC UNGUKA FINANCE Plc prioritizes the protection of personal data and takes all necessary measures to ensure that data is handled securely and in compliance with relevant data protection and privacy regulations. The bank implements technical, administrative, and physical safeguards to prevent unauthorized access, use, or disclosure of personal data. The following measures shall be put in place:

- LOLC UNGUKA FINANCE Plc shall employ cybersecurity practices and frameworks to safeguard the security of information of all data subjects in compliance with relevant cybersecurity regulations.

- Privacy by design will be embedded into the design and development of technology, systems, and practices.

- Projects with the potential to process personal data will undergo data protection impact assessments, with the assessments being approved by relevant stakeholders.

- Encryption, tokenization or pseudonymization requirements shall be integrated into the design and implementation of all applicable systems that process large amounts of personal data.

- where appropriate, storing sensitive personal data separately from other types of data.

This policy is passed and endorsed as fit to run and support the business of LOLC UNGUKA FINANCE Plc on 19th March 2024

Chief Executive Officer
Justin KAGISHIRO

Digitally signed by LUF(CHIEF EXECUTIVE OFFICER)
Date: 2024.08.28 12:19:55 +02'00'

Chairman of the Board
Yves SANGANO

Sign……

Digitally signed by LUF(CHAIRPERSON)
Date: 2024.10.15 12:13:33 +02'00'