P. O. BOX 75408 Kampala Uganda +256 312316900 | +256 393238278 www.fltug.com | info@fltug.com

DATA PROTECTION AND PRIVACY POLICY

Reviewed June 2024

Document Control

Owner	All Departments
Date Reviewed	25th June 2024
Date Approved	25th June 2024
Date of Next Review	25th June 2026
Approved By	Board of Directors
Classification	Internal Use Only
Version	2.0

Version History

The following revision history reflects all changes made to this document

Version	Date	Author	Description of Changes
1.0	25/06/2024		Second version

Document Approval

All parties involved acknowledge that they have read, understood and agree with all that has been specified in this document.

Name	Role	Signature & Date
Vincent Tumwijukye	Chief Executive Officer	 25th June 2024

Table of Contents

Policy details

1.0 Introduction

Futurelink Technologies (herein after referred to as “the company”) is committed to the proper handling of all personal and company data in its custody.

This policy defines the principles to be adhered to by the company’s staff and business partners to protect personal and organizational data collected, held, and processed by the Company.

Breach of this policy may lead to disciplinary action as deemed fit by the company’s leadership.

The policy has been written in accordance to the Data Protection Act of Uganda and the General Data Protection Regulation of the European Union (2016).

1.1 General Policy Statement

Individuals and systems responsible for the generation, transmission, storage, access and decommissioning of institutional data shall do so in a manner that preserves the rights of data subjects, guarantees that the data will be lawfully processed and ensures its Confidentiality, Integrity and Availability.

1.2 General Interpretations

In this policy unless the context otherwise requires;

Data: A collection of facts, such as names, age, measurements, observations, financial facts and descriptions of things or situations.

Personal data (and/or Personally Identifiable Information). data which relates to an individual who can be directly or indirectly identified from that data which includes a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Company data: Data that describes objects, systems, situations required for the day to day to day running of the company such as financial data, organizational inventory, email communication etc.

Institutional data: Means a combination of company data and personal data in the custody of the company’s employees and information systems.

Data subject: Means an individual from whom or in respect of whom personal information has been requested, collected, processed.

Data set: A group of data describing a common data subject

Data processing: Any operation or set of operations performed on institutional data, such as collecting, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data.

Data de-identification: Means the processing of personal data in such a manner that it can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identifiable natural person

Data Custodian: The person holding delegated authority from the Chief Executive Officer as one responsible for the management of data (responsibility and authority for defining the rights to collect, process, or store data) in a specific business function such as finance, human resources or Information technology. In the company's organizational structure, this role is held by a business process owner such as departmental head.

Data Breach: Unauthorized access, alteration or loss of data

System Owner or operator: The person responsible for the overall proper operation of a business system to serve organizational goals. The individual is a stakeholder in the security, data accuracy, procurement/development, integration, modification, operation, maintenance of the system and design of system specifications. In the company's organizational structure, this role is held by the Senior Manager Technology and Innovations.

Data processor or expert (internal or external): The person or system with the primary concern and technical capability to manipulate data into information or convert it from one form to another.

System User: Person or system that constantly interacts with institutional systems and data to achieve their day to day functions.

1.3 Scope

This policy is applicable to company data and personal data collected from the company's clients, employees and business partners. The policy is binding to all company employees and business partners that are involved in the generation, transmission, storage, access, safety and decommissioning of institutional data.

2.0 FILING OF COMPANY AND CLIENT'S DATA

2.1 Interpretation

Data filing is the systematic collection, organization and storage of institutional data. To ensure compliance to relevant regulations, safety, accuracy and usability of filled data, the following guidelines are to be applied

2.2 Principles

1. The company owns all institutional data collected, processed and stored by its employees and systems. Institutional data includes client and employee data stored and processed on organizational systems.
2. Only the data necessary to serve a clearly documented purpose shall be collected, a purpose that serves to satisfy a well-documented business objective or interest of the organization.
3. Data custodians are primarily accountable for the proper and lawful collection and filling of personal data sets. The data custodian shall hold a management role accountable for the security of the data during collection and filing whether it is collected in an automated or manual manner.
4. Data subjects will be fully made aware that their personal data is to be collected, updated, processed and shared for legitimate business purposes and shall give explicit consent to permit the company to do so.
5. For Personal data sourced from other sources other than the data subjects, the data custodian shall ascertain that the source of data complies with the appropriate/relevant data protection and management laws, .i.e. the Data Protection Act 2021 of Uganda and/or the General Data Protection Regulation of the European Union.

3.0 ACCESS TO INSTITUTIONAL DATA

3.1 Interpretation

Access to institutional data refers to the deliberate effort and ability to retrieve and view or process or transfer data. The following guidelines are to be referenced when accessing data or when granting date access permissions.

3.2 Principles

1. Access to institutional data shall be granted on a need to know basis. Only individuals that have a proven legitimate business or technical cause by virtue of their job description or role may be granted access.
2. Data subjects that directly contribute personal data to the company shall be permitted to access, update, erase, the data supplied.
3. Individuals permitted access to institutional data shall possess the knowledge and skills to safeguard this data and will be required to properly handle it in conformation with the company's Data Protection and Privacy Policy.
4. Systems that access, and process institutional data shall, by design, have appropriate measures in place to safeguard and process this data in a manner that conforms to the company's Data Protection and Privacy policy
5. The data custodian shall maintain an accurate log of the data access permissions for all data classified as "Restricted" by various systems and individuals
6. All (legitimate or otherwise) access, processing, erasure and disclosure of restricted data shall be tracked and logged. All suspected data breaches will be immediately reported to the data custodian and handled using the appropriate methods.
7. All data access rights shall be explicitly sought from the data custodian, the data custodian (or their delegate) possesses the responsibility to grant, deny and revoke access to institutional data.

4.0 THE STORAGE AND ACHIEVING OF INSTITUTIONAL DATA

4.1 Interpretation

Data storage is the process of retaining collected data for future use. Stored data is kept on various media types with the intent of using it soon and frequently. Archiving of data implies the storage of data for long term retention and less frequent access.

4.2 Principles

1. Institutional data shall be stored in a manner that ensures its Confidentiality, Integrity and Availability. Measures will be in place to safeguard this data from loss and illegal access, alteration and disclosure.
2. Data stored off the company's premises using cloud technologies or otherwise shall be in a location or country or under the custody of an organisation that has enacted privacy

policies/laws that are equivalent to the company's Data Protection and Privacy Policy or the GDPR of the EU or the Data Protection Act 2021 Act of Uganda.

3. Requests for data retrieval from archives shall be logged, auditable and approved by the data custodian. Requests such as these will be for legitimate purposes to satisfy business continuity or legal requirements.
4. Personal data shall be stored for a period only for which it is required for active business use or interest by the company. Personal data that the company no longer requires for purposes for which it was collected in the first place should be completely and permanently discarded.

5.0 DATA MIGRATION PROCESS FOR SAVINGS PLUS MANAGEMENT SOFTWARE

5.1 Interpretation

In this context, data migration is the process of legitimately moving personal and other data from the company's client system(s) such as a human resource or financial or banking system to the Savings Plus platform while preserving the integrity and meaning of the said data. The process typically involves data conversion to compatible formats and transfer into the Savings Plus platform.

5.2 Principles

1. All Data migration shall be done according to an approved plan by all stakeholders. All raw data shall be compiled by a client in accordance with approved data templates shared by the company.
2. All data submitted by clients shall be stored intact without alteration for future reference.
3. All data shall be shared by the client in a manner that proves such communication in future, and such communication must never be deleted.
4. The migration and verification processes shall be tracked and logged in an auditable format at every stage of performance to ascertain the completeness and accuracy of the data.
5. User Acceptance Testing, including data verification with submitted data, shall be done with the representatives of the company and the client, and evidence thereof shall be kept securely.
6. Precise parameters that define success or otherwise for each stage shall be clearly defined, agreed upon by the company's and the clients' data custodians and included in the migration plan prior to conversion, migration and verification.
7. The data migration process shall be performed in a designated downtime window following the

guidelines on management of downtime in section of the company's Technology Policy.

Where practical, snapshots/copies of client systems will be utilized in the conversion process.

6.0 GENERATION AND DESTRUCTION OF COPIES OF DATA

6.1 Interpretation

Generation of data involves the creation of raw data by collecting it from Data subjects or processing other raw data to produce more data. Destruction of data is the process of rendering data completely unreadable, unusable and inaccessible by humans or software. This section states principles that guide these processes for copies of organizational data.

6.2 Principles

1. The creation of physical and electronic copies of institutional data shall be restricted at a system and policy level to well documented business purposes and to users that already have legitimate access to the data.
2. Permission to copy or move or transform whole databases of institutional data from a business system or format to another shall be restricted to approved persons. Explicit permission to perform such actions shall be sought by personnel involved from the data custodian.
3. Data subjects that have directly contributed personal data to the company shall be permitted to instruct the organization to completely and permanently delete all active and archived personal data sets. An adequate mechanism shall be put in place to facilitate this process and to ascertain that the process has been fully executed within the limits of relevant laws and regulations of the country and the regulatory bodies such as banking and tax regulations.
4. Electronic and physical copies of data made for any purpose other than backup, shall be destroyed immediately after the purpose for which they were made, has been satisfied.
5. All institutional data shall be retained for a minimum of 10 years.

7.0 CONFIDENTIALITY POLICY

7.1 Interpretation

Data confidentiality refers to the state of data privacy; protection of restricted data from being accessed

or shared by un authorized persons or for unauthorized purposes. This section states the principles governing the processes of ensuring the confidentiality of institutional data.

7.2 Principles

1. Employees with access to institutional data shall by default and by design be required to maintain the highest level of confidentiality of this data.
   - Institutional data may only be disclosed to authorized persons or systems with prior approval of the data custodian.
   - A confidentiality clause shall be included in all types of staff employment contracts.
2. The company's business partners authorized to access and/or process institutional data are bound by the company's Confidentiality Policy and shall consent to a non-disclosure agreement.
3. The company's business and client systems shall be designed to provide assurance that the data held therein is kept confidential. They will be designed to prevent accidental disclosure of data using software development industry best practices and proper access rights and permissions.

8.0 DATA TRANSFER AND COMMUNICATION

8.1 Interpretation

Data transfer or communication is the process of exchanging data between persons or systems. Data may be exchanged within the company or between the company and its business partners as a routine under a running contract or as a one off. This section states the guidelines that govern this process.

8.2 Principles

1. Whenever possible, institutional confidential data shall be transferred using secure versions of communication protocols. In instances where confidential physical copies must be transmitted, a trusted courier (internal or external) with knowledge of the company's Data Protection and Privacy Policy will be employed.
2. Transfer of institutional data outside the company shall be justified and necessary. Only data relevant to the approved and justified well known business purposes or relevant legal requirements may be shared.
3. Personal data shared with external data processors shall be de-identified to the most logical extent possible. Recipient systems and persons should still be able to process the data and attain uncompromised results.

4. Institutional data shall only be shared amongst individuals or business partners that have been authorized by the data custodian to access the shared data. The recipient should be bound by the organizations Data Protection and Privacy Policy and/or the Data Protection Act of Uganda or the GDPR.
5. All Confidential Information shall be accessed by secured company devices
6. All institutional data shall be classified into three categories; Restricted, Internal and Public. Data explicitly classified as "Restricted" or "Internal" data is confidential and shall not be shared without prior approval. Data classified as "Public" is not confidential. All unclassified institutional data (electronic, physical or oral) is by default regarded confidential and should be treated as such unless the company has defined data as "Public".

9.0 DATA BACKUPS AND DATA RECOVERY

9.1 Interpretation

Backing up data implies copying of data to a secondary location for the purpose of safeguarding it from system failures or catastrophes. Data recovery therefore means the retrieval of the said data to its original usable state when required. This section states principles that govern this process.

9.2 Principles

1. All institutional data and systems shall be classified according to their criticality to business operations, continuity and excellence as "Critical", "Vital" and "Non-Critical". "Critical" systems and data shall be backed up daily with a "Low" Recovery Time Objective of at most 1 day. "Vital" systems and data shall be backed weekly with a "Medium" Recovery Time Objective of at most 1 week. "Non-critical" systems and data shall be backed up monthly with "High" Recovery Time Objective of at most 1 month.
2. For the benefit of doubt, **Crital** shall include all Banking as a Service B2B and B2C business systems, and company's financial data. **Vital** shall include all HR and Administration data. **Non-Critical** shall be defined from time to time.
3. A clear inventory of systems, services and data shall be maintained by system and process owners. The inventory shall document as much detail as is required to facilitate the efficient and effective back up and restoration of data in an unambiguous manner.
4. Backed up data shall be encrypted in transit and in storage
5. Backed up business-critical systems and data shall be stored at a location with no common underlying support systems (such as network connectivity, power supply) with the live

operational systems.

6. Back up data shall be access restricted to personnel directly involved in restoration procedures
7. Back up data shall be tested occasionally for completeness to ensure they are restorable well enough to restore a system back to an acceptable state to guarantee business continuity.
8. Backup and restoration procedures for critical systems shall be clearly documented and a copy of these kept separately from the main business operating environment.
9. Complete system image backups shall be performed at least once a month for highly critical systems to ensure their recovery can be performed with minimum effort and time