REPUBLIC OF KENYA

MINISTRY OF AGRICULTURE &
LIVESTOCK DEVELOPMENT

KENYA INTEGRATED AGRICULTURE MANAGEMENT INFORMATION SYSTEMS DATA GOVERNANCE FRAMEWORK

(KIAMIS)




For Data management and Dissemination

german cooperation

implemented by giz

Sweden Sverige

ASTGS 2019 2029

DIGITAL TRANSFORMATION CENTER KENYA

Food and Agriculture Organization of the United Nations

BETA

KENYA VISION 2030

ABBREVIATION AND ACRONYMS

ASDG	Agriculture Sector Data Gateway
ASTGS	Agricultural Sector Transformation and Growth Strategy
ATO	Agriculture Transformation Office
CAADP	Comprehensive Africa Agriculture Development Programme
CEC	Country Executive Committee
DGSC	Data Governance Steering Committee
DGTC	Data Governance Technical Committee
DPA	Data Protection Act
DPIA	Data Protection Impact Assessment
FDI	Foreign Direct Investment
GDPR	General Data Protection Regulation
GIS	Geographic Information System
GODAN	Global Open Data for Agriculture and Nutrition
GoK	Government of Kenya
ICT	Information and Communication Technology
ID	Identity Document
IT	Information Technology
JASSCOM	Joint Agricultural Sector Steering Committee
KESCoP	Kenya Statistics Code of Practice
KNBS	Kenya National Bureau of Statistics
KPI	Key Performance Indicators
M&E	Monitoring and Evaluation
MoALD	Ministry of Agriculture and Livestock Development
MoICT	Ministry of Information, Communications and Technology
ODPC	Office of the Data Protection Commissioner
SSF	Small-Scale Farmers
USSD	Unstructured Supplementary Service Data

Foreword

The modernization of Kenya's agriculture is aligned with the government of Kenya's Vision 2030, the global Sustainable Development Goals (SDGs), regional African Union Agenda 2063 and the Comprehensive Accelerated Agricultural Development Plan (CAADP); the EAC agricultural trade and food security treaties; the Kenya National Digital Master Plan 2022-2032, The National Climate Change Action Plan, 2023-27, ASTGS 2019-2029 and data protection act 2019.

Under Flagship 8 of the ASTGS, the MoALD has identified and prioritized data and digitalization as the key enablers that will facilitate the envisaged transformation and growth. In particular, BETA has prioritized data and digitally driven agriculture for speedy and more efficient, sustainable agricultural sector transformation through effective data management. To address the challenges of data MoALD is taking a bold step towards improving agricultural sector data collection, validation, analytics, and data sharing with a central database through KIAMIS with partnership with FAO and Sweden Embassy.

KIAMIS implementation started in 2029 with development of farmers' registration system and testing of the KIAMIS system. After successful testing, MoALD, working with FAO and Sweden Embassy, agreed to elaborate KIAMIS modules focusing on farmers' registration, E-voucher, e-extension & routine data hence promoting the need for the development of KIAMIS data governance framework. Effective data governance streamlines operations reduces costs, and facilitates secure data sharing, promoting transparency and accountability with the legal provisions of the Data Protection Act 2019.

The development of KIAMIS Data Governance Framework has followed the guidelines provided under the Data Protection Act, local and global agriculture and data access regulations and their best practices to establish the standards and protocols for data sharing across the agriculture landscape while also providing the guiding principles and policies for data collection, handling, processing, and quality assurance. As we launch this KIAMIS Data Governance framework, I hope that we rapidly adopt the defined implementation roadmap to enable the processes and systems for the exchange of Agriculture data. I therefore call upon all stakeholders in the sector to collaborate, align and implement the recommendations of this KIAMIS Data Governance Framework.

Signed by:

Dr. Andrew Karanja, PhD
Cabinet Secretary,
Ministry of Agriculture & Livestock Development

Acknowledgment

The Ministry of Agriculture and Livestock Development (MoALD) has developed KIAMIS Data Governance Framework to provide a comprehensive set of rules, processes, and standards that will enhance coordination in the agricultural sector's digital ecosystem, improving policy and management decisions through real-time data through Rolling-out farmer registration and e-subsidy management modules to counties, develop additional KIAMIS modules based on government priorities, Enhance human and institutional capacities for the system's operationalization and utilization at national and county levels and Strengthening coordination mechanisms and linkages for successful KIAMIS implementation at national and county levels in line with the Access to Information Act, 2016.

The journey towards the development of this Data Governance Framework has involved participation of several stakeholders at the national and county levels. The overall support and goodwill from the Cabinet Secretary, MoALD provided impetus and rallying call for key stakeholders to support the process. I wish to sincerely thank the leadership of key ministries, led by respective Principal Secretaries; namely: Jonathan Mueke, Principal Secretary, State Department for Livestock Development; Principal Secretary State Department for ICT and Digital Economy, Eng.John Tanui, MBS, Principal Secretary for Economic Planning; Mr. Alfred K'Ombudo, Principal Secretary for Irrigation Ephantus Kimotho, CBS; Dr. MacDonald George Obudho, EBS, Director General of the Kenya National Bureau of Statistics; Dr. Eliud Kiplimo Kireger, Director General of the Kenya Agricultural and Livestock Research Organization (KALRO). The office of the Data Protection Commission, led by Ms. Immaculate Kassait, MBS, was particularly instrumental in guiding the compliance with the Data Protection Act 2019.

We wish to thank the representatives of the Counties CECs for Agriculture; the private sector players led by CEO of ASNET, Dr Agatha Thuo; representative of universities and Tertiary Agriculture research Institutions, Dr. Muchelule Yusuf data governance expert; MOALD KIAMIS technical team who were instrumental in giving their inputs through participation and validations to its success. Finally we are grateful to our development partners; the Embassy of Sweden, Food and Agriculture Organization of the United Nations (FAO), World Bank, Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) and Tony Blair Institute for Global Change (TBI) for supporting the processes and finalization of this KIAMIS Data Governance Framework as we look forward to further more support for the adoption and implementation of this Framework.

Signed by:

Dr. Kipronoh Ronoh Paul (PhD)
Principal Secretary
State Department of Agriculture

TABLE OF CONTENTS

List of Figures

List of Figures

Definition of Terms

Agricultural Data: Information related to agricultural activities, including crop production, livestock management, fisheries, and cooperative activities.

Agriculture Sector Data Gateway (ASDG): The central repository for agricultural data in Kenya, providing a unified platform for data sharing, management, and access

Capacity Building: Activities aimed at enhancing the skills, competencies, and abilities of individuals and organizations in data governance.

Compliance: Adherence to laws, regulations, guidelines, and specifications relevant to data governance.

Data Architecture: The structural design of data systems and databases that ensures data assets are managed, secured, and utilized according to organizational objectives and regulatory requirements.

Data Custodian: Entity responsible for physically storing and maintaining the data infrastructure that houses data sets.

Data Governance Council (DGC): A central body responsible for providing strategic direction and oversight for data governance initiatives within the ministry.

Data Governance Secretariat: The body responsible for managing the day-to-day operations of data governance, including coordinating activities and monitoring progress.

Data Governance Technical Committee (DGTC): A committee that offers technical support and develops guidelines for implementing data governance policies and standards.

Data Lifecycle Management: Processes for managing data from creation and storage to archiving or deletion.

Data Owners: Individuals or entities responsible for specific datasets, ensuring their quality, security,control and compliance.

Data Protection Act: Legislation adopted to protect personal data and ensure privacy, including provisions for informed consent and privacy-by-design.

Data Quality Management: Procedures for data profiling, cleansing, standardization, and monitoring to maintain high data quality standards.

Data Security: Measures such as access controls, encryption, and regular security audits to protect data from unauthorized access and breaches.

Data Stewardship: The role of managing data quality and integrity, ensuring adherence to data governance policies, and facilitating data access and usage.

Data Validation: The process of ensuring that data is accurate, complete, and meets the required standards.

Feedback Mechanisms: Processes through which stakeholders provide input on data governance activities, enabling continuous improvement.

Implementation Tools: Software solutions that facilitate data governance activities, such as data catalogs, data quality tools, and metadata management systems.

Integration and Interoperability: Ensure data integration and interoperability acrossvarious systems.

Interoperability: The ability of different information systems, devices, or applications to connect and communicate in a coordinated way, within and across organizational boundaries.

Kenya Statistics Code of Practice (KeSCoP): This is a document that sets the professional standards that producers of official statistics must commit to when producing and releasing

official statistics

Metadata This is data that defines and describes other data; the data that provides information about one or more aspects of the data

Metrics and Reporting: Key performance indicators (KPIs) to measure the effectiveness of the data governance program and regular reports on data quality, compliance, and other governance metrics to stakeholders.

Ministry of Agriculture and Livestock Development (MoALD): The primary institution responsible for leadership, policy formulation, and coordination of data governance efforts in the agriculture sector.

Monitoring and Evaluation (M&E): The systematic tracking of the implementation and outcomes of data governance initiatives to assess their performance and impact.

Non-personal data on the other hand is data or information that cannot be used to identify a person. Often, data such as agronomic data (e.g., yield, nutrient, soil), machine data (e.g., fuel consumption, engine performance), and weather data is non-personal data and therefore is not governed by the Data Protection Act.

Performance Indicators: Specific, measurable metrics used to assess the success of data governance activities.

Personal data: It refers to any information relating to an identified or identifiable natural person. An identifiable natural person means a person who can be identified directly or indirectly, by reference to an identifier such as a name, an identification number, location data, and an online identifier or one or morefactors specific to the physical, physiological, genetic, mental, economic, cultural or social or social identity.

Policy Formulation: The process of creating policies, regulations, and standards related to data governance.

Reporting: The process of preparing and disseminating information on the status and progress of data governance activities to stakeholders.

Resource Mobilization: The process of securing financial, technical, and human resources required for implementing data governance initiatives.

Stakeholder Engagement: Involving relevant stakeholders, including government agencies, private sector partners, and farmers, in data governance and M&E activities.

Steering Committee (DGSC): A high-level body that provides strategic direction and oversight for data governance initiatives.

Technical Assistance: Support provided by IT and data management teams for implementing data governance initiatives and maintaining data security.

Technical Committee (DGTC): A group of experts providing technical support and developing guidelines for data governance implementation.

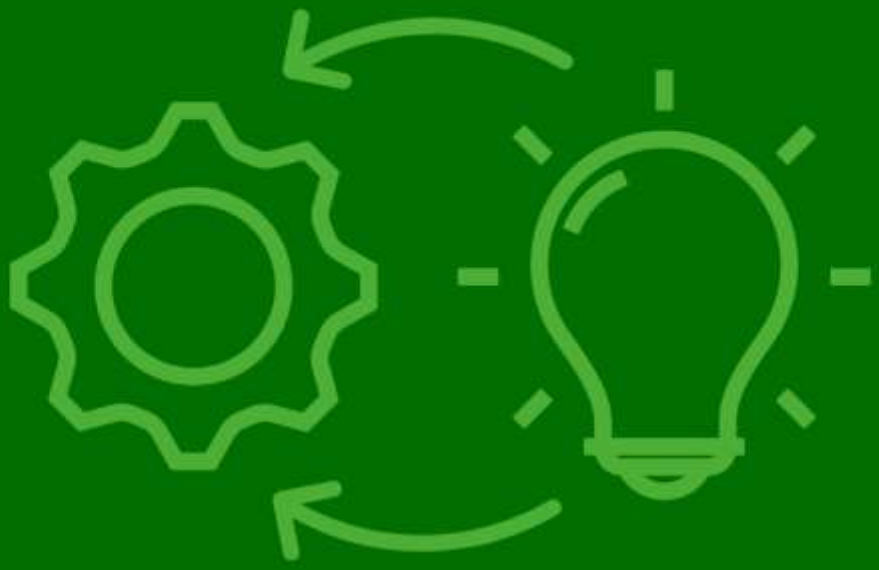
Executive Summary

The Data Governance framework has been developed to establish guidelines, processes, and responsibilities to ensure data quality, stewardship, data protection, security, accountability, transparency, and compliance for effective data sharing, management, and dissemination on the Ministry of Agriculture and Livestock data assets. The framework emphasizes alignment with regulatory requirements such as Kenya's Data Protection Act 2019; as it incorporates international data protection standards to facilitate global operations and build stakeholder trust by promoting integrity and trust in line with BETA pillars and United Nations sustainable development goals. To support the implementation of the ASTGS Flagship on data and innovation, the framework builds upon already existing policies and guidelines in Kenya and beyond and encompasses five central governance pillars.

- *The first pillar is on governance structure,* and the framework outlines defined roles and responsibilities for data management. Key institutions include; the **Ministry of Agriculture and Livestock Development (MoALD)** whose key role will be to provide overall leadership and oversight for the implementation of the data governance framework. The Ministry will ensure alignment with national policies and strategies, formulate policies, regulations, and standards related to data governance in the agriculture sector, and coordinate and collaborate with other government agencies, development partners, and stakeholders to harmonize data governance efforts;
- *The second pillar* of this framework *is on Data Quality Management*: The framework is tryingto ensure data quality is essential for informed decision-making by including procedures for data profiling, cleansing, standardization, and monitoring to maintain high data quality standards across the MoALD. These are governed by the Data Protection Act adopted in 2019.Six key data privacy standards such as informed consent and privacy-by-design are outlined, and their applications discussed
- *The third pillar is about Data Security and Privacy and aims at* protecting sensitive data. Theframework proposes measures such as access controls, encryption, and regular security auditsto safeguard data from unauthorized access, breaches, and compliance violations.
- *The fourth pillar addresses Data Lifecycle Management* and aims at managing data throughoutits lifecycle for efficiency and compliance. The framework encompasses hands-on tools and practices that help individuals and entities apply policies and guidelines for data creation, storage, usage, archival, and disposal, adhering to regulatory requirements and industry best practices.
- *The fifth pillar of the framework tackles* questions regarding Compliance and Regulatory Alignment proposes the establishment of key processes and procedures for data management and provides guidance on how to address them. By adhering to these principles, the MoALD can optimize data use, support informed decision-making, maintain compliance with regulatoryrequirements, and protect stakeholder interests.

The benefits accrued to the implementation of this framework include reliable and high-quality data to support informed decision-making at all levels of the MoALD; enhanced Security and Compliance with data protection; robust security measures and compliance adherence mitigating risks associated with data breaches and regulatory violations; increased Efficiency

due to standardized processes and clear responsibilities streamlining data management, reducing redundancies and improving productivity; Improved Stakeholder Trust through demonstrating commitment to data governance among stakeholders to foster stronger relationships and reputation; Innovation Enablement with Well-managed data assets provide a foundation for innovation, enabling the development of data-driven solutions and strategies. Implementation of this Data Governance Framework will enable the Ministry to effectively manage, protect, and leverage its data assets. This Data Governance Framework provides a comprehensive approach to address key aspects of data governance, fostering a culture of data excellence and driving success in key Ministry's objectives and goals.



CHAPTER ONE:

INTRODUCTION

Provides background on the Ministry of Agriculture and Livestock Development's (MoALD) role in advancing Kenya's agricultural sector. It explains the objectives of the Data Governance Framework (DGF), focusing on data-driven innovations to enhance service delivery in the sector.

CHAPTER ONE: INTRODUCTION

1.1 Background

The Ministry of Agriculture and Livestock Development (MoALD) is at the forefront of Kenya's efforts to modernize its agricultural sector, playing a pivotal role in the implementation of the Agricultural Sector Transformation and Growth Strategy (ASTGS) 2019-2029. The ASTGS seeks to create a vibrant, competitive, and commercially oriented agricultural sector that achieves 100% food security, enhances productivity, increases producer incomes, and boosts household food resilience, all within the context of Kenya's devolution process. KIAMIS Data Governance Framework (DGF) supports the implementation of the ASTGS, particularly through Flagship 8 of the strategy. This flagship, titled "Research, Innovation, and Data", focuses on the role of data and digital innovation in enhancing the agricultural sector's research capabilities and in driving improved decision-making processes. It emphasizes:

- Farmer profiling, to better understand the needs of small-scale farmers, pastoralists, and fisher folk.
- The creation of a digital central farmers' database, which integrates multiple agricultural use cases under a single system to improve access to critical data.
- Data-driven innovations that enhance service delivery to farmers, ensuring transparency, efficiency, and better-targeted interventions.
- The development of digital tools and platforms that enable the seamless exchange of data across the agricultural ecosystem, facilitating collaboration among government agencies, counties, and private stakeholders.

In line with the Bottom-Up Economic Transformation Agenda (BETA), agriculture is one of Kenya's top five key economic pillars. By leveraging data-driven agriculture, the sector can undergo a rapid and sustainable transformation. This transformation is underpinned by Kenya's progress in ICT development, internet connectivity, and the widespread use of mobile technology, although challenges remain in terms of data management. Recognizing the critical need for high-quality agricultural data, MoALD is working to address the challenges of data availability, quality, and sharing. The Kenya Integrated Agriculture Management Information System (KIAMIS) plays a central role in managing this data. KIAMIS is designed to:

- Harmonize data collection across the agricultural sector.
- Provide a single depository for agricultural data, serving as the single source of truth for agricultural statistics in Kenya.
- Improve data sharing among stakeholders, including county governments, private sector players, research institutions, and development partners.

In summary, the Data Governance Framework provides the necessary structures and processes to support the ASTGS by ensuring that data is treated as a strategic asset. By establishing clear guidelines for data governance, the framework fosters a data-driven agricultural sector that can address the challenges of food security, productivity, and sustainable growth in Kenya. Through effective data management, the framework will enable better planning, monitoring, and evaluation of agricultural programs, ultimately contributing to the overall success of the ASTGS. This extended introduction provides a more detailed overview of the relationship between MoALD, ASTGS, and the role of data governance in supporting Kenya's agricultural transformation. It also highlights the importance of digital solutions and the legal frameworks that guide the use of agricultural data.

1.2 Objectives

KIAMIS Data Governance Framework serves multiple objectives, all aimed at improving data management within the agricultural sector. These objectives include:

- **Baseline for Harmonized Data Management:** The framework sets out clear rules and processes to ensure consistency and standardization in how data is collected, processed, stored, and shared. This reduces duplication of efforts, ensures data quality, and promotes collaboration between stakeholders.
- **Understanding Current Data Management Practices:** By creating a shared understanding of current data management practices, the framework helps stakeholders identify gaps and inefficiencies in existing systems. This facilitates the improvement of these systems over time.
- **Ensure Data Accuracy and Reliability:** The framework emphasizes the importance of KIAMIS data accuracy and reliability. By implementing comprehensive data quality management protocols, the framework aims to ensure that all agricultural data is up-to-date, complete, and fit for decision-making purposes.
- **Protection of Sensitive Data:** One of the core objectives of the framework is to protect sensitive agricultural data, particularly personal data collected through the Kenya Integrated Agriculture Management Information System (KIAMIS). This includes safeguarding personal information from unauthorized access, breaches, or misuse, in full compliance with the Data Protection Act of 2019.
- **Facilitate Seamless Data Access:** The framework aims to strike a balance between making agricultural data accessible to stakeholders and maintaining appropriate data security controls. This ensures that authorized entities have access to the data they need while preventing unauthorized access or breaches.
- **Support Evidence-Based Decision Making:** Reliable, high-quality data is critical for making informed decisions at all levels of the agricultural sector. The framework provides a structure to ensure that agricultural data can support policies and strategies aimed at improving food security, enhancing productivity, and boosting rural incomes.
- **Ensure Adherence to International Standards:** The Data Governance Framework is aligned with international best practices in data governance, including standards outlined in the General Data Protection Regulation (GDPR) and United Nations

Sustainable Development Goals (SDGs). This enhances Kenya's global standing in data management.

- **Promote Accountability and Governance:** The framework fosters a culture of accountability among stakeholders responsible for agricultural data management. By defining clear roles and processes, it ensures that data management practices are transparent and that data is treated as a valuable public asset.
- **Enable Innovation through Data:** High-quality, well-managed data can drive innovation in the agricultural sector. The framework encourages the development of digital tools and solutions that use data to solve challenges faced by farmers, agro-dealers, and policymakers. This includes innovations in areas like predictive analytics, supply chain optimization, and market access

1.3 Scope of KIAMIS Data Governance Framework

The Data Governance Framework (DGF) applies comprehensively to all agricultural data managed under the Kenya Integrated Agriculture Management Information System (KIAMIS). KIAMIS is the central platform for collecting, processing, storing, and sharing agricultural data across Kenya. The scope covers a broad range of agricultural datasets, including those related to:

- **Crop production:** Data on crop yields, varieties, production areas, and crop performance across various regions of Kenya.
- **Livestock:** Information on livestock numbers, health status, breeding, production systems, and trade.
- **Fisheries:** Data on fishing activities, aquaculture, fish production, and market trends within Kenya's fisheries sector.
- **Market information:** Price data, demand and supply trends, value chains, and agricultural trade, both domestically and internationally.

Weather and climate data: Meteorological data, climate change indicators, and information on drought, rainfall, and other environmental factors affecting agriculture

`1.4 Data Collection and Lifecycle Management

The framework governs the entire data lifecycle from data collection, storage, and analysis, sharing, to archiving or destruction. It provides protocols for:

- **Data Collection:** Standardized processes for gathering data through surveys, remote sensing, and routine data entry from field officers, farmers, and other sources.
- **Data Processing:** Guidelines for cleaning, validating, and transforming raw data into usable formats.
- **Data Storage:** Ensures secure and compliant storage of data in KIAMIS, supported by the Big Data Centre at KALRO.
- **Data Archiving:** Outlines the procedures for long-term retention of data and criteria for archiving datasets that are no longer in active use.
- **Data Destruction:** Policies for safely disposing of data after it has reached its retention limit, in accordance with the legal and operational requirements.

1.5 Data Ownership and classification

KIAMIS framework establishes clear ownership and classification protocols for agricultural data:

- **Data Ownership:** The Ministry of Agriculture and Livestock Development (MoALD) is designated as the data controller, with ultimate responsibility for agricultural data managed in KIAMIS. Other stakeholders, such as county governments and private sector entities, act as data processors.
- **Data Classification:** Agricultural data is classified based on sensitivity and access level, such as public data, restricted data, and confidential data. This classification determines who can access, process, or share the data and under what conditions.

1.6 Data Governance Principles

The Data Governance Framework (DGF) is built on key principles that ensure the effective management, security, and utilization of agricultural data within KIAMIS (Kenya Integrated Agriculture Management Information System). These principles are crucial for maintaining trust, ensuring data quality, and facilitating collaboration among stakeholders. The principles outlined below form the foundation for the responsible and sustainable governance of agricultural data:

a) Accountability: Accountability is the cornerstone of the Data Governance Framework, ensuring that clear roles and responsibilities are assigned to all stakeholders involved in data management. This principle guarantees that:

- Data Controllers (such as MoALD) and Data Processors (counties, private sector partners) are aware of their obligations in managing, storing, and processing data.
- Specific individuals or departments are held accountable for the accuracy, security, and integrity of data within KIAMIS.
- Data Stewards are appointed at various levels to oversee data governance policies and ensure compliance with standards.

This principle ensures that any issues related to data (such as breaches, errors, or delays) are traceable to specific roles, which improves decision-making and ensures that corrective actions can be taken swiftly.

b) Transparency: Transparency within the DGF promotes open documentation of all data management processes, making sure that every aspect of data handling is:

- **Visible and Auditable:** Data governance activities, such as data collection, storage, processing, and sharing, are documented to allow for internal and external audits. This enhances trust among stakeholders, as it demonstrates how data is managed responsibly.
- **Traceable**: Every action related to data is recorded, ensuring that data can be tracked throughout its entire lifecycle, from collection to destruction. This traceability provides an audit trail that can be used to identify potential issues or inconsistencies in the data management process.
- **Accessible:** Documentation regarding data governance policies, standards, and procedures is made available to relevant stakeholders, ensuring that everyone understands how data is managed and what their responsibilities are.

Transparency fosters an environment where stakeholders are confident in the integrity of the data being used for decision-making, planning, and research.

c) Integrity: Maintaining the accuracy, completeness, and consistency of data is

essential for the framework. The principle of data integrity ensures that:

- **Data Accuracy:** Data is collected and processed accurately, reflecting true values across various agricultural activities (crop production, livestock, fisheries, etc.). Processes such as data validation and data cleansing ensure that errors are identified and corrected early in the data lifecycle.
- **Consistency:** Data remains consistent across different systems, ensuring that there are no discrepancies between datasets. For example, data entered at the county level aligns with national-level data within KIAMIS.
- **Data Quality:** The integrity of data is preserved through stringent quality control mechanisms, ensuring that only reliable and verified data is used for policy formulation, research, and other agricultural activities.

By adhering to this principle, the DGF ensures that decisions based on data are made on accurate and trustworthy information, enhancing the overall effectiveness of agricultural programs.

d) Compliance: The DGF ensures strict adherence to national and international legal frameworks governing data management. The most significant regulation in this regard is the Data Protection Act 2019, which outlines:

- **Data Privacy:** Personal data collected from farmers and other stakeholders is handled responsibly, with measures such as informed consent, data minimization, and data anonymization in place to protect individuals' privacy.
- **Legal Requirements:** The framework ensures that all data governance activities comply with the legal requirements set out in the Constitution of Kenya 2010, Access to Information Act 2016, and other relevant policies.

Compliance with these regulations ensures that the data is handled in an ethical, lawful, and secure manner, minimizing the risk of data breaches and other violations. Additionally, compliance fosters international partnerships, as the data governance framework aligns with global standards.

e) Sustainability: The framework is designed to be adaptive and future-proof, ensuring that data governance processes can evolve alongside changes in technology, policy, and agricultural needs. Sustainability is achieved through:

- **Scalability:** KIAMIS and the data governance processes are built to handle increasing volumes of data, making them scalable as Kenya’s agricultural sector grows and more data is collected.
- **Flexibility:** The framework is flexible enough to accommodate new technologies and data sources, ensuring that it remains relevant in an ever-changing digital landscape.
- **Long-Term Vision:** By focusing on sustainable data management practices, the framework ensures that data governance activities are not just short-term solutions but are embedded within the long-term strategies of MoALD and other stakeholders.

This adaptability ensures that the framework can respond to emerging trends, technological advancements, and changing regulatory requirements while continuing to deliver value to the agricultural sector.

1.7 Roles and Responsibilities

The framework specifies the roles and responsibilities of different stakeholders involved in data management, ensuring a collaborative approach:

- **National Government (MoALD):** Leads the overall governance and management of agricultural data, ensuring compliance with national policies and strategies.
- **County Governments:** Responsible for data collection and local management of agricultural data, working in close collaboration with MoALD to ensure consistency across regions.
- **Private Sector:** Involved in using and contributing to data through partnerships, innovation, and the development of agricultural technologies and services.
- **Research Institutions:** Contribute to data analysis and validation, ensuring that data is used for evidence-based policy formulation and agricultural research.
- **Development Partners:** Support data governance initiatives by providing technical assistance, funding, and capacity building
- **The Data Governance Council (DGC)** provides strategic oversight, ensuring that data governance policies align with national priorities.
- **The Data Governance Technical Committee (DGTC)** offers technical guidance on data standards and quality control.
- **The Data Governance Secretariat** handles the day-to-day management of data governance processes. These roles are clearly delineated to ensure smooth collaboration between stakeholders, prevent duplication of responsibilities, and enhance accountability.

1.8 Communication and Training

Effective communication and training are critical to the success of the DGF. The framework includes programs aimed at raising awareness among stakeholders, including government officials, private sector partners, and farmers, about their roles in data governance. Training programs focus on building the technical capacity of data managers and other stakeholders, ensuring they have the skills needed to manage and use agricultural data effectively.

CHAPTER TWO:

Legal and Regulatory Framework:

Discusses the legal context governing agricultural data in Kenya, including the Constitution, the Data Protection Act 2019, and various acts related to agriculture and fisheries. It also outlines compliance requirements for handling personal and non-personal data.

CHAPTER TWO: LEGAL AND REGULATORY FRAMEWORK

2.0 Introduction

This chapter focuses on the institutional, legal and regulatory frameworks underpinning the KIAMIS Data Governance Framework (DGF), essential for managing agricultural data effectively. It outlines how data is sourced, stored, integrated, and secured, while also discussing the regulatory context governing data management in Kenya.

2.1 LEGAL AND REGULATORY FRAMEWORK

2.1.1 The Constitution

Chapter Four, Article 35(1) of the Constitution provides that every citizen has the right of access to:

a) Information held by the State; and
b) Information held by another person and required for the exercise or protection of any right or fundamental freedom.
c) Articles 35 (3) further provides that the state shall publish and publicize any important information affecting the nation. In addition, the right to privacy is provided under Article 31 (c) of the Constitution outlines the right of every person not to have information relating to family or private affairs unnecessarily required or revealed.

The Fourth Schedule of the Constitution states that data collection is a shared responsibility between the national and county governments – where the national government is responsible for national coordination, collection of national-related data/information; data policy, legal framework, guidelines/standards and capacity building; and county governments are responsible for collection of county-based data. The development of KIAMIS gives the Government overall mandate to collect agricultural data and information as a public good to be given to the citizen as envisaged in the Constitution. The government, at both national and county levels, take lead in design and management of KIAMIS as a shared responsibility for data collection in line with the Fourth Schedule.

2.1.2 Access to Information Act, 2016

This Act of Parliament enacts Article 35 of the Constitution and holds the government of public entity as foremost responsible for collecting and providing information that may be demanded by the citizen. The Act specifies the rights of Citizens to get reliable, accurate information and specifies penalties for non-compliance. Further, under Section 17 on Management of records (1) In this section, "records" means documents or other sources of information compiled, recorded or stored in written form or in any other manner and includes electronic records.

In Section (2), the Act states that every public entity or Ministry shall keep and maintain—(a) records that are accurate, authentic, have integrity and useable; and (b) its records in a manner which facilitates the right of access to information as provided for in this Act. Section (3) further states that at a minimum, to qualify to have complied with the duty to keep and maintain records under subsection (2), every public entity (ministry) shall create and preserve records (data) necessary to support policies, decisions, procedures, transactions and other activities pertinent to the Ministry's mandate; ensure that the records are maintained in good order and condition; and computerize the records using information management systems in order to facilitate more efficient access to information. In line with Access to Information Act 2016, KIAMIS has been designed to collect accurate, reliable, timely data and information;

to establish and maintain a central database records, with the records kept in formats to facilitate data accessibility.

2.1.3 Statistics Act 2006

The Act provides for the establishment of the Kenya National Bureau of Statistics (KNBS) as the overall government agencies that handles and coordinate official statistics in Kenya. The Act further mandates KNBS to collect, compile and publish certain data and statistics, while Section 4(g) of the Act provides that one of the objectives of KNBS is to collaborate with and assist the Ministries, Departments, Agencies, Counties and any other institutions in the production of official statistics. Section 4(j) of the act further states that KNBS shall designate statistics produced by National Statistical System as official statistics on being satisfied that the necessary criteria have been followed.

2.1.4 The Crops Act 2013

The objective of the Act is to, "accelerate the growth and development of agriculture in general, enhance productivity and incomes to farmers and the rural population, improve investment climate and efficiency of agribusiness and develop agricultural crops as export crops that will augment the foreign exchange earnings of the country, through promotion of the production, processing, marketing and distribution of crops in suitable areas of the country." An efficient system with the relevant data is required to achieve the said objectives. Section 3(d) of the Act further states the objective of the Act is to reduce duplication and overlap of functions among institutions involved in the coordination and regulation of crops activities.

2.1.5 Fisheries Management and Development Act (No. 35 of 2016)

Section 9 of the Act established three Kenya Fisheries Service (KFS); the functions of the KFS include: to collect and analyse data in relation to resources and activities falling within the scope of this Act. Section 75 of the Act mandates KFS to collect and manage any information and data, including information relating to fishing, fisheries, aquaculture, landing, research, storage, food safety, processing, buying, selling, exports and other related transactions. KIAMIS system handles fishing and aquaculture data collection and management with the office of KFS involved in handling all the fisheries data.

2.1.6 The Agriculture and Food Authority Act No. 13 Of 2013

Section 4 of the Act: states among others, the functions of AFA being to collect and collate data, maintain a database on agricultural products excluding livestock products, documents and monitor agriculture through registration of players as provided for in the Crops Act.

2.1.7 The Agricultural Sector Transformation and Growth Strategy (ASTGS) 2019-2029

The Agricultural Sector Transformation and Growth Strategy (ASTGS) 2019-2029 is a comprehensive strategy being implemented by the MoALD and Counties to guide the transformation and growth of the agricultural sector. Among the pillars of the ASTGS is the use of data and digitalization as key enablers of the envisaged agricultural transformation. KIAMIS data governance framework implementation is aligned to ASTGS and is the tool being used to deepen the data agenda while also supporting the digitalization of farmers' support services and products.

2.1.8 The Agriculture Policy 2021

This Policy provides a framework for sustainable development of the Agricultural Sector and outlines effective guidelines for efficient use of opportunities and resources available in the

Sector and provides for inter-linkages of agricultural support systems such as irrigation, extension, infrastructure and research. The Policy also provides a basis for mainstreaming food and nutrition security concerns in the country's development programmes and plans. To address the data gaps, the policy states that:

a) The National and County Governments will;

- Ensure that agricultural census is conducted every ten years.
- Promote use of ICT in crops, livestock and fisheries services to improve communication and data management and sharing.
- Support establishment & management of agricultural sector data and information database for planning, research and effective implementation of programmes.

b) The County governments will:

- Support & develop mechanisms to continuously collect, collate and share agricultural sector information and data with the National Government & its key stakeholders.
- Support provision of timely and reliable information on farmer's registration, e-voucher, routine data, e-extension, transactional data & reporting.

2.2 Regulatory Environment concerning sharing of Personal Data

While agricultural and livestock data is not generally considered as 'personal data,' there are certain data types such as the farmers names or mobile number that are personal. Other data types such as the GPS location or photos of farmers and farms that can reveal personal identity are also considered as personal data. It is important that agricultural data sharing is compliant with existing legal framework.

2. 2.1 The Data Protection Act, 2019

The most critical legislative instrument governing the sharing and usage of data of personal data and that informs the design and implementation of the Data Governance Framework is the **Data Protection Act 2019 (DPA)** which regulates the processing of personal data and the protection of data subjects' privacy rights. The DPA stresses that every data controller or processor (e.g. agro-dealers, government agencies like the MoALD, and any other actors collecting and processing data) must ensure:

- Lawfulness, fairness, transparency, Integrity and confidentiality
- Purpose limitation, i.e., processing personal data for explicit, specified, and legitimate purposes.
- Provide the data subject with valid explanation whenever information relating to family or private affairs is required.
- Accuracy. Personal data should be up to date and reasonable steps should be taken to ensure that any inaccuracy is erased or rectified without delay.
- Storage limitation, i.e., personal data should not be kept for periods longer than the purposes it was collected for.
- Personal data is not transferred outside Kenya unless there is proof of adequate data protection safeguards or consent from the data subject.

These principles have become known as the **Data Protection Principles** (section 25 of the DPA). Looking at the regulated actions covered by the DPA, the following can be outlined:

- Type of data to be collected and their Security

- Disclosure, accuracy, udating and retention of data

The DPA provides for the Rights of Data Subjects as follows:

- To be informed of the use to which their personal data is to be put. This means that data subjects have the right to be provided with clear and concise information about how their personal data will be used.
- To access their data in the custody of the MoALD, the Data controller.
- To object to the processing of all or part of their data.
- To rectify personal data. The MoALD is required to rectify false or misleading information without undue delay relating to their data subjects.
- To erasure. This means that if a data subject no longer wants their personal information to be stored or processed by the MoALD, they have the right to request its deletion.

There are **eight legal bases for the lawful use of personal data.** The data processors and controllers have to consider;

- The data subject consents, contractual purposes
- To be compliant with a legal obligation and For legitimate interests
- For the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- For the performance of any task carried out by a public authority
- For the exercise, by any person in the public interest, of any other functions of a public nature; to the harm and prejudice to the rights and freedoms or legitimate interests of the data subject; or
- For historical, statistical, journalistic, literature and art or scientific research.

Finally, another important element in the collection and processing of personal data under the DPA is asking the question of who the data controllers are and who are the data processors of the personal data. The law recognizes that not all organizations involved in processing personal data have an equal level of responsibility.

Obligations of a data controller under DPA 2019:

- The data controller must exercise overall control over the purpose for which, and the way, personal data is processed. Therefore, activities such as interpretation, the exercise of professional judgment, or significant decision-making concerning personal data.
- The data controller is responsible and must demonstrate compliance with the eight aforementioned principles relating to the processing of personal data (duty of accountability).
- The data controller is also responsible for the compliance of their data processor(s). For instance, MoALD should consider the vendors they engage and ensure that they opt only for a data processor who provides sufficient guarantees that processing will meet the requirements under the Act and protect data subjects' rights.
- The data controller is legally responsible for the processing of personal data and is liable for any damage caused by the processing and in case of a data breach.
- Must be registered with ODPC as a data controller.

- Must ensure implementation of appropriate technical and organizational measures to ensure effective implementation of data protection principles and necessary safeguards in data processing. MoALD must consider privacy and data protection issues at the design phase of any system, service, product, or process and then throughout the lifecycle.
- The data controller must conduct Data Protection Impact Assessments where the processing is likely to result in a high risk to the rights and freedoms of data subjects.
- Data Controllers have to report personal data breaches to the ODPC without delay within 72 hours of becoming aware of the breach.

Obligations of data processors under DPA 2019:

- The data processor's main responsibility is to process the personal data it receives strictly based on the instructions of the data controller. The data processor will also need to take all measures to protect and safeguard personal data to ensure data security, including protection against accidental or unlawful destruction or loss, alteration, unauthorized disclosure, or access.
- The data processor should demonstrate compliance with the eight aforementioned principles relating to the processing of personal data.
- The data processor cannot bring in another processor without authorization from the controller. In addition, a data processor who, without lawful excuse, discloses personal data processed without the prior authority of the data controller commits an offence.
- A data processor involved in the processing of personal data is liable for damage caused by the processing only if the processor — (i) has not complied with an obligation under the Act specifically directed at data processors; or (ii) has acted outside, or contrary to, the data controller's lawful instructions.
- Notification of personal data breaches. If a data processor becomes aware of a personal data breach, they must notify the relevant data controller within 48 hours. A data processor must also assist the data controller in complying with its obligations regarding personal data breaches.

2.2.2 Aligning the KIAMIS Data Governance Framework with the Data Protection Act 2019

The MoALD and Counties will ensure that KIAMIS data collection, database management and data sharing comply with the regulations provided under the Data Protection Act 2019. This will be done by:

- Ensuring that KIAMIS system and modules takes into account the principle of "Data protection by design or by default"
- Ensuring that all the agricultural data actors at national and county levels register with the office of Data Protection Commission as data controllers and processers;
- Every data controller or data processor to implement appropriate technical and organisational measures which are designed— (a) to implement the data protection principles in an effective manner; and (b) to integrate necessary safeguards for that purpose into the processing.
- All the data controllers and data processors shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which is

necessary for each specific purpose is processed, taking into consideration— (a) the amount of personal data collected; (b) the extent of its processing; (c) the period of its storage; (d) its accessibility; and (e) the cost of processing data and the technologies and tools used.

- When collecting and sharing personal data, all the data controllers and processor shall consider measures such as— (a) to identify reasonably foreseeable internal and external risks to personal data under the person's possession or control; (b) to establish and maintain appropriate safeguards against the identified risks; (c) to the pseudonymisation and encryption of personal data; (d) to the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (e) to verify that the safeguards are effectively implemented; and (f) to ensure that the safeguards are continually updated in response to new risks or deficiencies.
- Where the data processing involves the transmission of data over an information and communication network, all the data controllers shall have regard to— (a) the state of technological development available; (b) the cost of implementing any of the security measures; (c) the special risks that exist in the processing of the data; and (d) the nature of the data being processed.
- Where any of the data controller is using the services of a hired vendor— (a) the data controller shall opt for a data processor who provides sufficient guarantees in respect of organisational measures to protect personal data; and (b) the data controller and the vendor shall enter into a written contract which shall provide that the vendor shall act only on instructions received from the data controller and shall be bound by obligations of the data controller.
- All the data controllers and processors shall take all reasonable steps to ensure that any person employed by or acting under the authority of the data controller or data processor, complies with the relevant security measures.

CHAPTER THREE:

KIAMIS Infrastructure and Architecture:

Details the Kenya Integrated Agriculture Management Information System (KIAMIS), including its infrastructure and architecture. It emphasizes the design principles to support agricultural data management.

CHAPTER THREE: KIAMIS INFRASTRUCTURE AND ARCHITECTURE

3.0 Introduction

The effectiveness of a governance framework relies heavily on data infrastructure and architecture, ensuring that data assets are managed, secured, and utilized according toMoALD objectives and regulatory requirements. The infrastructure and architecture play a crucial role in enforcing governance policies, ensuring regulatory compliance, and mitigating risks associated with datamanagement. The chapter explains the key data governance framework infrastructures and architecture required for successful DGF implementation as follows: -

3.1. KIAMIS Infrastructure

The KIAMIS data infrastructure supports data governance by furnishing essential hardware, software, and networking components to securely store, process, and transmit data. It facilitates the implementation of security measures, access controls, and monitoring mechanisms to safeguard data integrity and confidentiality.

- KIAMIS system hardware & Softwares
- **Storage Systems:** Should be in compliance with government guidelines in data storage systems either virtual or physical.
- **Computing Resources:** Sufficient computing resources should be allocated based on the expected workload, technical consideration, policies, and legal requirements
- **Big Data Centre at KALRO**
- **Networking Infrastructure:** Network Protocols: Standardized rules and regulations for transmitting data over networks. Common network protocols include TCP/IP, HTTP/HTTPS, FTP, SSH, and DNS.
- **Security and Compliance:** To enhance regular data forensics and audits compliance with specified standards and regulations such as the Data Protection Act 2019.

3.2 KIAMIS Data Architecture

The data architecture defines the framework for data collection, storage, processing, and access within the ministry. It encompasses the design of data systems, databases, flows, and models, establishing the structure and organization of data assets. KIAMIS has a thoughtfully crafted and executed data architecture that empowers the ministry and stakeholders to effectively leverage its data assets, driving value from data and supporting data-driven decision-making processes.

3.3 Design of KIAMIS system

- Description of KIAMIS database & data workflows

KIAMIS Data Storage:

- Determine the appropriate storage mechanisms for different types of data based on factors such as access patterns, scalability, performance requirements, and cost considerations.
- Common storage options include relational databases (e.g., MySQL, PostgreSQL), NoSQL databases (e.g., MongoDB, Cassandra), data warehouses (e.g., Amazon Redshift, Google BigQuery), and data lakes (e.g., Hadoop HDFS, Amazon S3).

KIAMIS Data Integration:

- Establish mechanisms for integrating data from various sources and formats within specified data sets across various stakeholders both internally and externally.

KIAMIS Data Models:

- Design data models that represent the structure, relationships, and constraints of the MoALD's data entities.
- Develop conceptual, logical, and physical data models to provide a blueprint for database design and implementation.
- Consider techniques such as entity-relationship modelling, dimensional modelling, and schema normalization/de-normalization.

KIAMIS Data Access and Analytics:

- Provide various mechanisms for data access, analysis, visualization and reporting.
- Consider the needs of various user groups and applications for accessing and consuming data, and design appropriate data access layers and APIs.

KIAMIS Scalability, Performance, and Resilience:

- Enhance data systems architects to handle data volumes growth, backups, user concurrency, and system failures.
- To utilize distributed computing paradigms, replication, caching, partitioning, storage, and load balancing techniques to achieve scalability and fault tolerance.

KIAMIS Data Security and Privacy:

To safeguard data sets against unauthorized access, breaches, vulnerabilities, and threats, robust security controls must be implemented. These controls should encompass both technical and procedural safeguards to ensure comprehensive protection. Access to all data formats should be strictly limited to authorized personnel only, employing stringent authentication mechanisms and access controls.

Adequate ICT infrastructure is essential, supported by accompanying policies and practices designed to uphold the security and integrity of data throughout their transmission and storage processes. This includes encryption protocols, firewalls, intrusion detection systems, and regular security audits to identify and address potential vulnerabilities proactively. In the event of any breaches in privacy and security, swift remedial actions must be taken following the existing legal framework. Penalties should be applied where applicable to deter future incidents and uphold accountability. Continuous monitoring, updates to security protocols, and staff training programs are vital components of maintaining a robust data security posture

CHAPTER FOUR:

KIAMIS Data Management Processes:

Explains the types of agricultural data handled, including farmer profiling, production data, and food security information. It also covers data collection methods, quality control, and storage processes.

CHAPTER FOUR: KIAMIS DATA MANAGEMENT PROCESSES

4.0 Introduction

Effective data governance framework starts with the established processes and methods as well as tools and systems put in place to collect and process data throughout the data lifecycle. The data collection and processing methods also take into account measures to ensure data quality and reliability. This chapter delves into the types of data, data collection and management, as well as data quality measures in existence under KIAMIS, or planned to be effected in the near future.

4.1 Types of agricultural Data

The agricultural data are categorized into many types:

- **Category by methods of data collection;** eg Census data, farmers' registration data, surveys data, administrative data; expert estimates data; GIS/ remote sensing/ satellite and other earth observation tools data
- **Category by sub-sector grouping:** eg crops, livestock, fisheries, irrigation, trade, food security, agroforestry, land use, population data
- **Category by value chain:** from inputs to production, post-harvest losses, access to finance, farm assets, market prices, markets access, farm earnings, value addition, and processing, farmers' advisory services; adoption of technologies; transactional data; soil quality data; agro-meteorology data; early warning data; risks mitigation, insurance data, and water quality data.

In line with KIAMIS guidelines, the agricultural dataare categorized as follows:-

4.1.1 Farmers profiling, mapping and registration data

- Farmer profiles: bio-data on the characteristics of the farmer, age, gender, personal identification, etc
- Mapping: taking the GPS locations of farms, mapping farms
- Registration data: Keeping farmers' register in a safe central database for use.

4.1.2 Agriculture Production Data

- Crops, livestock and fisheries products
- Production Indices: area, yields, numbers,
- Value of Agricultural Production

4.1.3 Food Security and Nutrition Data

- Suite of Food Security Indicators,
- Food Stocks Balances and Supply Utilization Accounts

4.1.4 Trade Data

- Crops, livestock and fisheries products local sales; exports, imports
- Trade Indices

4.1.5 Commodity Prices Data

- Producer Prices, Wholesale and retail prices
- Consumer Price Indices, Deflators and Exchange rates

4.1.6 Land, Inputs, and Sustainability Data

- Land use data, cover area
- Land Use for agriculture at national & county levels
- Land under irrigation, reclaimed land, wasteland, idle land and rangeland
- Irrigation potential, national and subnational
- Water resource development and potential for irrigation

4.1.7 Agricultural Inputs data

- Fertilizers by Nutrient and by product
- Livestock Manure
- Seeds and seedlings
- Semen & Fingerlings
- Pesticides Use and trade
- Animal feeds, Drugs & vaccines
- Tools, equipment, and machinery

4.1.8 Sustainability Indicators

- Cropland Nutrient Balance
- Livestock population trends and diversity
- Fish stock status

4.1.9 Climate Change Indicators

- Temperature change

4.1.10 Population and Employment Data

- Census data, Farmers registration data

- Rural and urban farming population

4.1.11Agricultural Employment Indicators

- Employment Indicators: Agriculture
- Employment Indicators: Rural

4.1.12 Agricultural Investment Data

- Government Expenditure on agriculture, Credit to Agriculture
- Development Flows to Agriculture and Foreign Direct Investment (FDI) in agriculture

4.1.13 Macroeconomic Indicators

- Macro Indicators, Capital Stock & Climate Change: Agrifood systems emissions

4.1.14 Environment/Greenhouse Gas Emission Indicators

- Emissions indicators from livestock (enteric and manure management) and crops(aggregated sources)
- Absolute emissions, Emissions intensities and Land use change

4.2 Data Collection Methods

The following methods are used for data collection;

4.2.1 Census of Agriculture

- Periodicity: Carried out every ten years
- Methodology: complete enumeration of all farm holdings
- Collected indicators: structure of agriculture, baseline data
- Legal mandate: KNBS
- Challenge: high cost/ expensive

4.2.2 Farmers Registration Data

- Periodicity: Carried out once and thereafter continuously
- Methodology: complete enumeration of all farmers
- Collected indicators: profiling, mapping baseline data
- Legal mandate: MoALD and Counties
- Challenge: Sustainability of continuous registration

4.2.3 Agricultural Surveys

- Periodicity: Carried out every season; quarterly; annually
- Methodology: Sampling enumeration of data sources
- Collected indicators: Outputs and input data; other data as required by the Ministry and Counties
- Legal mandate: Ministry and Counties (under the support and supervision of KNBS)
- Challenge: high cost/ expensive

4.2.4 Administrative, Routine data

- Periodicity: Carried out every day, every week, every month
- Methodology: Taking of official transaction records, data submitted from sources by legal instruments; data collected by field extension officers through expert estimates
- Collected indicators: Mostly inputs, activities, and outputs data
- Legal mandate: Ministry, Counties and state corporations

- Challenge: Many gaps

4.2.5 Use of GIS, satellite, and remote sensing tools

- Periodicity: Carried out every day, every week, every month
- Methodology: Use of GIS, drone technology and Earth Observation tools; other emerging methods eg machine learning, and Artificial intelligence;
- Collected indicators: Mostly those that can be observed from above and complement the traditional data collection methods
- Legal mandate: Ministry, Counties and state corporations
- Challenge: Limited skills

4.3 Data Quality Control

4.3.1 Data Quality Management

Data quality management involves implementing comprehensive practices and procedures throughout the entire lifecycle of data from collection, analysis, storage, and dissemination; with the primary aim of ensuring that data is of high quality and effectively meets the needs of its users.

Quality in statistics is a multidimensional concept about the process, output, and the institution that produced the data. As a best practice, all producers of agricultural data and statistics shall adhere to the Kenya Statistics Code of Practice (KeSCoP) and consider the following 10 quality dimensions throughout the entire data lifecycle. Producers shall also inform users on compliance of data and statistics of each of these dimensions and their appropriateness as fit for purpose.

4.3.2 Data Quality Dimensions

- **Relevance**: The degree to which statistical information meets the real or perceived needs of users. This dimension of quality addresses how useful the data/statistics are for the issues that are important to users, and producers must prioritize the most important needs of their users.
- **Methodological Soundness:** This is the extent to which the methodology used to compile statistics complies with the relevant international standards, including the

professional standards enshrined in the UN Fundamental Principles for Official Statistics.

- **Accuracy:** The closeness of computations or estimates to the unknown exact or true values that the statistics were intended to measure. This can be expressed in terms of quantitative measures of accuracy, including possible sources of error such as coverage, sampling, non-response and response error rates; or qualitative assessment indicators.
- **Reliability:** This refers to the closeness of the initial estimated value to the subsequent estimated value. Consistently large differences between subsequent estimates to an initial estimate suggest possible bias in the initial estimate, while random large gaps between subsequent estimates and an initial estimate may indicate a need to re-assess the timeliness of subsequent estimates.
- **Timeliness:** This is the length of time between data availability and the event or phenomenon they describe." This references both:
    - the time lapse between the end of a reference date/period for data collection and receipt of the data for compilation and processing (timeliness of source data), and the time lapse between the end of a reference date/period and data dissemination(timeliness of output).
- **Punctuality:** This is closely associated with timeliness and is the "time lag between the actual delivery of the data and the target date when it should have been delivered." This relates to whether or not data are disseminated on scheduled release dates.
- **Accessibility:** This is the ease and conditions under which statistical information can be obtained. This relates not only to how easily data can be accessed by users but also to the form the data are in and the means through which users have access to the data.
- **Clarity:** The extent to which easily comprehensible metadata are available, where these metadata are necessary to give a full understanding of statistical data to the users.
- **Coherence:** This is the degree of adequacy of statistics to be combined in different ways and for different uses. It refers to comparisons between statistics for the same or largely similar populations." Coherence in statistics is the degree to which the data constitute a logical picture of the population they are describing.
- **Consistency:** This refers to statistics having logical and numerical coherence.

4.3.3 Data Quality Assurance

Within KIAMIS framework, the MOALD will undertake Data Quality Assurance (DQA) as a critical process to ensure the data accuracy, completeness, reliability, and integrity of data used in the Ministry, Counties, State Corporations, projects and programmes. The following measures will be taken as part of the DQA:

- **Data Profiling:** After every data collection process, team of statistics and ICT experts shall undertake basic analysis of the existing databases to understand its structure, content, and interrelationships. This will help in the identification of anomalies, training data, outliers, missing values, or duplicates.
- **Data Cleansing:** After data profiling, the team of experts shall proceed to data cleaning. This involves detecting and correcting (or removing) of wrong, corrupt or inaccurate data. To do this, experts from various thematic groups shall provide relevant edit specifications..

- **Data Validation:** Before sharing the cleaned data, the statistics and ICT experts will be required to undertake data validation. This involves taking measures to ensure that the final meets the required standards before it is used. To undertake the validation, the experts will use different techniques including frequency analysis, pattern recognition, format checks, and cross-field validations by confirming the output data with external interest groups.
- **Master Data Management (MDM):** After data cleaning and validation, the experts managing KIAMIS data shall proceed to ensure that the Ministry is able to link all the critical data to a common point of reference by centralizing the master data and synchronizing data across all systems.. This will ensure data consistency and accuracy across different systems and data sources.
- **Data Interoperability:** During data processing, KIAMIS officials will be expected to undertake measures aimed at ensuring that different systems within the Ministry and government in general, or software applications are configured to facilitate access, exchange, interpretation and use of data seamlessly and effectively. This will ensure that data can be shared across diverse systems without loss of context, meaning, or integrity, enabling meaningful collaboration and integration across various platforms and sectors.

4.3.4 KIAMIS Metadata Management

All data and statistics produced by KIAMIS will have accompanying standardized metadata that provides context, such as data source, date of collection, and data quality indicators defining the underlying concepts and definitions of the data collected and statistics produced, the variables and Classifications used, the methodology of data collection and processing, and indications of the quality of the statistical information in general, sufficient information to enable the user to understand all of the attributes of the statistics, including their limitations. The KIAMIS metadata will be documented and used according to internationally accepted standards with accompanying guidelines and procedures.

4.4 Data Storage

All the KIAMIS datasets and databases shall be kept at the Ministry's Big Data Centre stationed at KALRO head office. The Big Data Centre has sufficient server capacity and all the data centre infrastructure with assured continuous power supply, anti-fire, among others. For regular backups KIAMIS has put in place data recovery systems and procedures.

4.5 Data Usage

The overall goal of data collection is to make use of the data for decision-making, and supporting the operational activities.

Every cycle of data collection will end with process of data retrieval and querying, data processing and transformation, data analysis, visualization, and reporting. While processing data for use. The key factors to take into account shall include data accuracy, relevance, timeliness, and user access permissions.

4.6 Data Sharing and Distribution

KIAMIS data sharing has three levels of protocols, namely, internal data sharing, Counties data sharing and external stakeholders' data sharing. Moreover, there are two main types of data sharing, namely Open data sharing and personal/sensitive data sharing. Appendix B provides the Guidelines for Data Sharing.

4.7 Data Archiving and Destruction

To ensure effective use of KIAMIS, MoALD will archive data by moving data that is no longer actively used to a separate storage location for long-term retention. In this regard, the KIAMIS backend team shall be tasked to identify and categorize data for archiving based on usage and retention Guidelines. The Data archiving will also be done in line with the Kenya Archives regulations.

4.8 Data Incidence Management

Data Incidence refers to any event or occurrence that may affect KAIMIS data integrity, availability, confidentiality, or quality of data. The causes of data incidents may include data breaches , data lost accidentally, and unauthorized access to data corruption, hardware failures, accidental deletions, ransomware attacks that encrypt data without a decryption option, software bugs, malware infections, system crashes, privilege escalation attacks, stolen credentials or any anomaly that compromises the reliability and security of data.

Duplicate records, missing values, incorrect data entries, or outdated information; inappropriate or unauthorized use of data in ways that violate policies, laws, or ethical guidelines; human error such as mistakes made by individuals, such as misconfigurations, accidental deletions, or improper handling of sensitive data; cases of cyber-attacks, such as malicious activities by hackers or cybercriminals aimed at stealing, corrupting, or disrupting data; disaster events such as data lost due to floods, fires, or earthquakes that can damage data storage systems and result in data loss.

CHAPTER FIVE:

Data Governance Implementation Framework:

Focuses on the steps for implementing the DGF, including defining roles for various institutions and creating committees to oversee data governance at both national and county levels.

CHAPTER FIVE: DATA GOVERNANCE IMPLEMENTATION FRAMEWORK

5.1 Introduction

A data governance framework is a structured set of policies, procedures, roles, and standards designed to ensure the effective management and use of an organization's data. It establishes guidelines for data quality, security, ownership, and compliance, providing a systematic approach to managing data assets and supporting organizational goals. This process includes developing and enforcingpolicies, standards, and procedures to ensure data quality, security, and compliance. It involvesassigning roles and responsibilities for data stewardship, creating mechanisms for data monitoring and reporting, and fostering a culture of data accountability and transparency. The goal is to manage data as a valuable resource, enabling effective decision-making, operationalefficiency, and regulatory compliance.

5.1.2 General Goals of a Framework

Data governance iscrucial for ensuring the quality, security, and proper management of an organization's data. It enhances decision-making by providing reliable and accurate data, ensures compliance with data protection laws, and protects sensitive information.

An effective data governance framework will:

- Provide clarity on roles and responsibilities
- Establish rules for data use (e.g., collection and sharing)
- Minimize the risks of collecting, storing & using data
- Help meet regulatory expectations
- Improved decision making
- Improved communication

5.1.3 Data Governance Framework Essentials

- Data Architecture: The structural design of data systems and databases implementation
- Data Governance Implementation Tools: Software solutions that facilitate data governance activities, such as data catalogues, data quality tools, and metadata management systems.
- Data Governance Metrics and Reporting:
    - Metrics: Key performance indicators (KPIs) to measure the effectiveness of the data governance program.
    - Reporting: Regular reports on data quality, compliance, and other governance metrics to stakeholders.

5.2 Data Governance Framework Implementation

5.2.1 The Five Pillars of Data Governance Implementation

Applying the concept of a data governance framework to agriculture sector data, five central pillars can be highlighted, which form the baseline for well-functioning data governance:

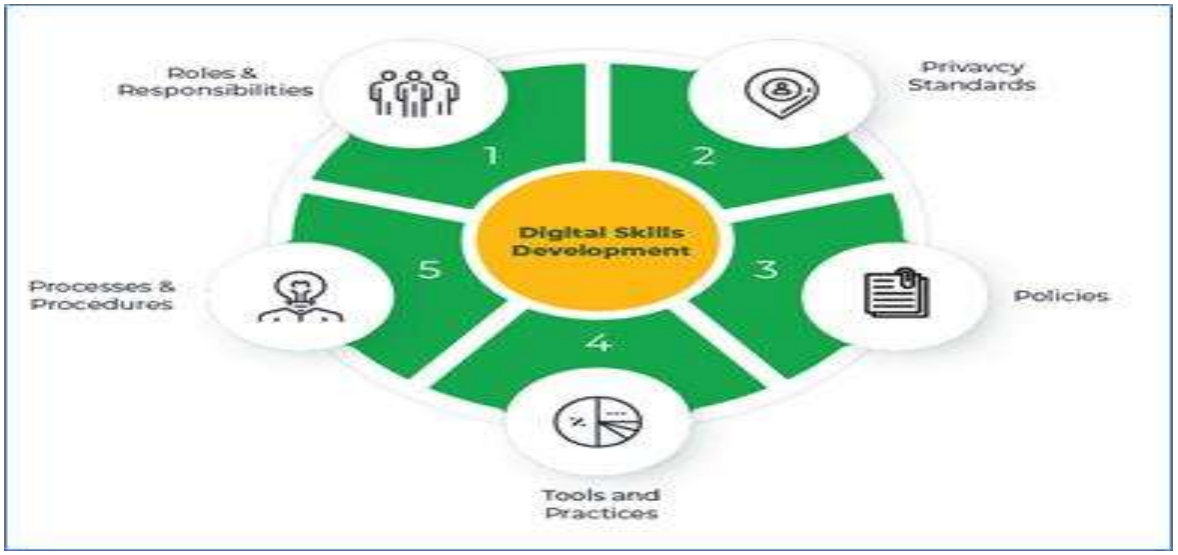


Figure 1: Showing Data Governance Pillars

- **Assigning Roles and responsibilities:** Data stewards, data managers and editors, data handlers and data experts are the backbone of every data governance framework. The right attribution of these roles and responsibilities ensures that data is accurately collected, turned into interoperable quality data sets, uploaded in time onto the preferreddata sharing platform, and processed and accessed in compliance with relevant privacyand security standards. Investing heavily in the training and education of these key personnel is essential.
- **Alignment with the Regulatory environment for collecting and processing data:** As elaborated in section 4, ensuring the legal basis for using and sharing agriculture sector data is the foundation to leverage data responsibly and confidently for better decision-making and innovation. There are also six additional data privacy standards toensure that the collection and processing of farmers' registration data is in line with the Data Protection Act, namely, (i) ensuring informed consent, (ii) applying privacy-by- design, (iii) complying with data subjects' rights, (iv) breach notification and (v) the appointment of Data Protection Officers.
- **Adopting Relevant Policies and guidelines:** The core purpose of policies and guidelines around agriculture sector data is to recognize that it is a critical asset and must be treated as such. Relevant policies and guidelines that need to be developed under this pillar are (i) an internal data governance policy, (ii) an external (open) data policy, (iii) internal data protection and security guidelines, as well as (iv) a data retention policy.
- **Tools, practices and Standards:** The first set of tools encompasses instruments to safeguard the personal data of farmers, namely, (a) information on how to anonymize and pseudonymize data, (b) a data protection impact assessment (DPIA), (c) best practices on data minimization, as well as (d) an informed consent template. The secondset of instruments centers on facilitating the sharing of farmers' data. To address the challenges of business- to-business (B2B) and business-to- government (B2G) data sharing, is discussed and provided. It helps set common standards for data- sharing andprovides principles that the signatories agree to apply in their data sharing contracts.
- **Processes and procedures for data management:** Mapping processed data is essential in relation to data flows, actors, and activities, from data collection to data sharing (Standard Operating Procedure format). These processes and standards includedefinitions of how data

will be stored, moved, changed, accessed, and secured. Mechanisms to monitor data quality need to be established as well.

IT and Data Management Teams

These teams ensure that data governance practices are effectively executed through reliable and secure technical systems.

Their main functions of the IT and Data management teams are proposed as follows: -

- Technical assistance for implementing data governance initiatives.
- Implementing and maintaining robust data security measures.
- Managing data infrastructure and storage solutions.
- Ensuring data integration and interoperability across various systems.
- Assisting in the development and deployment of data governance tools and technologies.

5.2.2 Key steps in the implementation of a Data Governance Framework

- Developing a common understanding
- Alignment with the regulatory framework
- Setting up the relevant management structures
- Tools, Procedures, Guidelines & Training
- Developing and executing a roadmap

5.3 Institutional Framework

MoALD Data Governance Framework establishes the roles, responsibilities, and relationships among various entities involved in data governance within the Ministry of Agriculture and Livestock Development (MoALD). This framework is crucial for ensuring effective data management, fostering accountability, and promoting collaboration among stakeholders. Below is a detailed summary of the institutional framework as described in this document?

5.3.1 Key Institutions and their Roles

Ministry of Agriculture and Livestock Development (MoALD)

- Leadership and Oversight: MoALD provides overall leadership and oversight for the implementation of the data governance framework. It ensures alignment with national policiesand strategies.
- Policy Formulation: Responsible for formulating policies, regulations, and standards related todata governance in the agriculture sector.
- Coordination: Coordinates with other government agencies, development partners, and stakeholders to harmonize data governance efforts.

5.3.2 Proposed KIAMIS Data Governance Institutional Framework

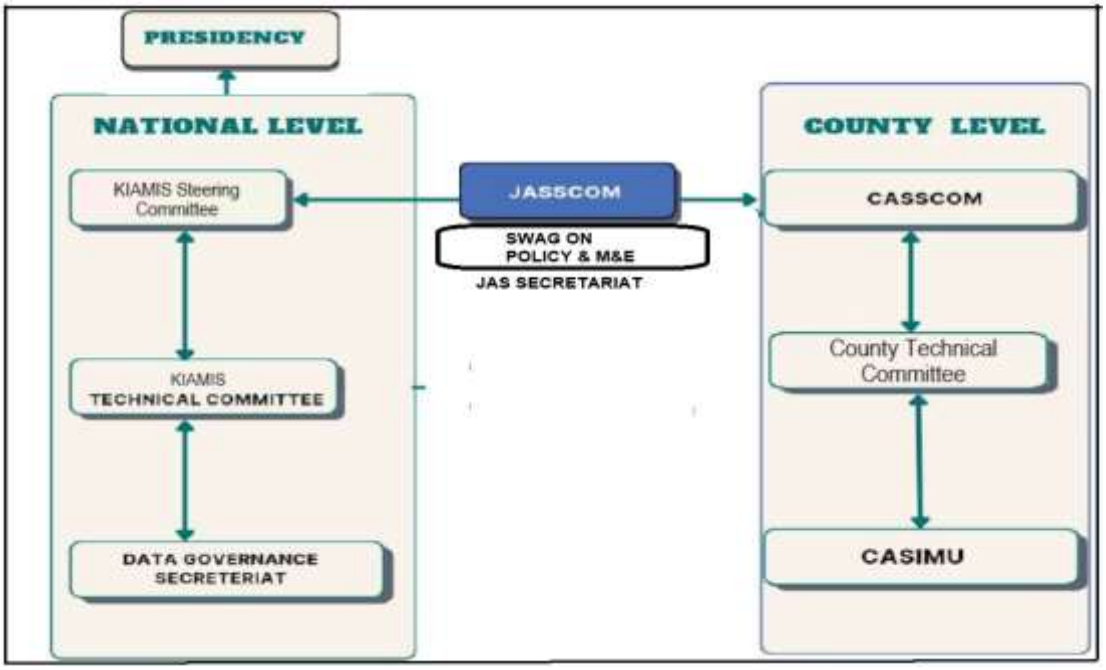


Figure 2: Data Governance Coordination Structure

5.3.3 AT NATIONAL LEVEL

5.3.3.1 The Presidency

The office of the President and Deputy President will be directly involved in the farmers registration exercise.

The roles include: Overall coordination and oversight; provision of strategic policy direction, resource mobilization from state and non-state actors; fostering of harmonious relations between the national and county governments.

5.3.3.2 Data Governance Council (DGC)/ KIAMIS Steering Committee

The committee will be formed at the national level by the cabinet secretary for Agriculture and Livestock Development. It will comprise Principal Secretaries for Agriculture, livestock development, Ministry of ICT, Ministry of Interior and any other government agency. Office of the data protection, the Chair of the National Farmer's Association, the representative of development partners and representative of the private sector,representative of the Council of Governors. Custodian of data is the Cabinet Secretary in the Ministry of Agriculture and Livestock Development. The DGC members will be appointed by the Cabinet Secretary for Agriculture and Livestock Development. Cabinet Secretary, MoALD will be the chair of the Data Governance Council.

Roles

- **Policy Development:** Creating and maintaining data governance policies, standards,and procedures to ensure data quality, consistency, and security.
- **Strategy and Vision:** Establishing the strategic vision for data governance and aligning it with the organization's overall business objectives.
- **Approval of Data Stewardship:** Designating data stewards who are responsible for

implementing and enforcing data governance policies within their respective areas.

- **Compliance and Risk Management:** Ensuring that the Ministry and key stakeholders comply with relevant regulations and standards and managing data-related risks.
- **Data Quality Management:** Establishing processes for maintaining high data quality, including data accuracy, completeness, and reliability.
- **Issue Resolution:** Addressing and resolving data-related issues, such as data ownership disputes or data quality problems.
- **Education and Awareness:** Promoting data governance awareness and providing training to employees about their roles and responsibilities in maintaining data integrity and security.
- **Performance Monitoring:** Monitoring and reporting on the effectiveness of data governance initiatives and making adjustments as needed.

5.3.3.3 KIAMIS Data Governance Technical Committee (DGTC)

It will comprise of the following Directors from Agriculture, livestock development, Irrigation, Fisheries, Cooperative, Lands, trade and Environment, Heads of ICT from Agriculture and Livestock , Heads of Statistics from Agriculture and Livestock, KNBS, Agricultural representatives from COG, JASSCOM, Development partners, Private sector, Researchers/Tertiary institutions, CEC Caucus, Data protection officer, Director of the communication unit. The Permanent secretary of Agriculture will be the chair and convener. The DGTC will be appointed by PS for Agriculture in consultation with the PS of Livestock.

Roles:

- **Technical Support:** Offers technical support and expertise in the implementation of data governance policies and standards.
- **Guideline Development:** Develop technical guidelines and tools for data management, ensuring adherence to best practices.
- **Capacity Building:** Provides training and capacity-building programs for stakeholders involved in data governance.
- Monitor and evaluate data governance performance.

5.4 Data Governance Secretariat

It will be composed of representatives from the Agriculture and Statics Unit from Agriculture and Livestock, representatives from the Department of ICT in the Ministry of Agriculture and Livestock Development, and ATO. The Secretariat will be appointed by the two PS State Department for Agriculture and PS State Department of Livestock.

Data Governance Secretariat Roles:

- Operational Support: Manages the day-to-day operations of the data governance framework,
- Coordinate implementation of activities and monitor progress.
- Stakeholder Engagement: Facilitates communication and collaboration among Stakeholders to ensure effective implementation of data governance
- Support and facilitate operations of DGC and DGTC
- Liaise with County Data Governance Technical Committee (CDGTC)

- Ensure compliance with policies and standards.
- Reporting: Prepares and submits regular reports on the status and progress of data governance activities to the DGC and DGTC.

5.5 Council of Governors

It comprises of the county governor as the chair and the CECM agriculture as the secretary; with other counties CECM and chief officers with overall County Agricultural coordination and oversight mandate.

Roles

- Coordinate county agriculture sector stakeholders and provide strategic policy direction,
- Fostering of harmonious relations between the national and county governments while liaising with DGTC on data governance issues
- Facilitate adoption and implementation of data governance policies and guidelines
- Technical Support: Offers governance policies and standards.

5.6 AT COUNTY LEVELS

5.6.1 CASSCOM (County Agricultural Sector Steering Committee

CASSCOM is anchored on Legal Notice (No. 2 of 2012) on Establishment of Joint Committees in Agriculture Sector under (Intergovernmental Relations Act) 2012: CASSCOM (County Agricultural Sector Steering Committee) is structured to oversee agricultural activities and ensure effective coordination within Counties. CASSCOM's comprises of Chief Officers, County commissioner; relevant directors , agriculture sector program/ project coordinators; A representative of the financial institutions operating in the county; A representative of the farmers' organizations; A representative of the private sector umbrella organization; A representative of a key Value Chain Umbrella organization; A representative of development partners , NGOs and PWD's in the county with the roles of coordinating agricultural operations, promoting key value chains, strengthening farmer organizations, and maintaining updated agricultural data registers in line with DGTC key roles at county level.

Roles

- Establish multidisciplinary structures for coordination of agricultural sector in counties
- Develop instruments for operation and accountability of the coordination structures
- Foster collaborations and linkages with public and private institutions in the management and delivery of agricultural programs and services
- Support implementation or development of Policies/ strategies/ regulations/ plans/ legislations of relevance to sector compliance with legal frameworks related to data management.
- To develop and approve Food security strategies and investment plans
- Registration and regulation of agricultural extension service providers to provide advisory support to the county government on agricultural matters

- Delegate it's mandates to relevant organs within CASCOM and set up any Ad-hoc sub-committee or task force for the sole purpose of executing a specific assignment on its behalf as need may arise; and
- To consider, harmonize, approve and review joint work plans, memoranda of understanding (MOUs); agreements, contracts, public private partnerships for programs and projects in the sector as well as providing a comprehensive link to the JASSCOM at the National level

5.6.2 KIAMIS County Technical Committee

Proposed membership:

- All county directors responsible for agriculture: crops, livestock, fisheries, Irrigation, Cooperatives, Marketing/trade, Agribusiness, Veterinary;
- County KNBS officer
- County Coordinators of data supporting projects eg NAVCDP, FSRP
- Representative- County ODPC & Members of CASIMU

Roles

- Develop the roadmap for KIAMIS implementation at County level, covering issues of data collection, database management, data governance and data sharing processes
- Oversee the technical implementation of prioritized modules and activities as prioritized and approved by the CASSCOM.
- Developing criteria for the selection of priority data and digital support services
- Coordination of data and digital agriculture stakeholders to eliminate duplication of efforts and silo activities at county level
- Advising the CASSCOM on all technical aspects of KIAMIS
- Lead the technical aspects of KIAMIS Institutionalization within the County

5.6.3 County Data Governance Secretariat (CASIMU)

It comprises of county data officers and county ICT officer.

CASIMU operates under the guidelines of the Ministry of Agriculture and Livestock Development. The purpose of CASIMU is to centralize and streamline data collection, management, and dissemination related to agriculture within the county, ensuring alignment with both county and national planning frameworks.

Roles

- Engage with various stakeholders, including private sector entities, government agencies, and farmers. They organize routine meetings to discuss data sharing, management, and utilization.
- They continuously monitor the progress of data governance initiatives, ensuring adherence to established policies and timelines .
- Support to Data Governance Council (DGC) and Technical Committee (DGTC): supports these bodies by providing technical and operational support, facilitating their meetings, and implementing their directives at the county level
- Liaison with County Data Governance Technical Committee (CDGTC): acts as a liaison, ensuring smooth communication and coordination between the county and national

governance structures .

- Ensure compliance with data governance policies, including adherence to the Data Protection Act 2019. They oversee the safe handling and sharing of data, maintaining data privacy and security standards .
- Data Quality and Security: They implement measures to maintain data quality, integrity, and security, including the management of a secure data infrastructure.
- Training and Capacity Building: supports training programs for county staff and other stakeholders, enhancing their capabilities in data management and governance.

5.6.4 Joint Agriculture Sector Steering Committee (JASSCOM)

JASCOM was created to provide regular direction for sector transformation initiatives agreed between the two levels of government (National and county), and follows-up upon Intergovernmental Forum meetings. A specific role of the JASSCOM is to oversee the functioning of the Joint Agriculture Intergovernmental Secretariat (JAS-IGS) and the Sector Technical Working Groups **– (**SWAGs) to ensure that decisions and resolutions are circulated to and implemented by relevant entities within the two levels of government. JASCOM are vital for maintaining data integrity, quality, and compliance within the ministryby facilitating consultations and cooperation between national and county. Agricultural transformational office links with JASCOM through data governance council (DGC)

5.6.5 Data Owners/Controller

Data Owner/controller is the Cabinet Secretary, MoALD,. The CS is responsible for ensuring the data is managed, used, and protected in alignment with the organization's strategic objectives and regulatory requirements.

Roles and responsibilities:

Overseeing data management within their units, ensuring data supports business operations and objectives, and allocating resources for data-related activities.

Developing data governance policies, ensuring data aligns with business strategy, and managing data-related risks and opportunities.

- Overseeing data management from a technical perspective, ensuring data infrastructure supports data governance policies, and integrating data governance with IT strategy.
- Managing data relevant to their functional areas, ensuring data quality and compliance, and making decisions about data access and usage within their jurisdictions.
- Ensuring product-related data is accurate, secure, and used effectively to improve product performance and customer satisfaction.
- Managing project-related data, ensuring it is used appropriately to achieve project goals, and maintaining data quality and security.
- Ensuring data management practices comply with relevant laws and regulations, managing data privacy and protection, and mitigating legal risks associated with data sharing.

5.6.6 Data Stewards

Data Stewards shall be data subject matter experts who understand both the business and technical aspects of data they manage. They shall ensure that KIAMIS Data Governance Framework is successfully implemented by focusing on data quality, compliance, and proper usage, Data Stewards shall help maximize the value of data as a strategic asset while minimizing risks associated with poor data management. The Stewards will be: data and statistics officers in the Ministry, state corporations and counties; ICT officersdealing with data systems and database management.

Roles and Responsibilities:

- Data Quality Management: Ensuring that data is accurate, complete, and reliable. This involves data cleansing, validation, and regular monitoring to identify and resolve data quality issues; Implementing data quality rules, conducting data audits, and monitoring data quality metrics.
- Maintaining metadata, which includes descriptions, definitions, and context of data elements. This helps ensure that data is well-documented and easily discoverable; Creating and updating metadata repositories, ensuring metadata accuracy, and promoting metadata standards.
- Policy Implementation: Enforcing data governance policies, standards, and procedures established by Data Owners and the DGSC; Ensuring compliance with data governance policies, training staff on data governance practices, and monitoring adherence to policies.
- Ensuring that data is used appropriately and in compliance with relevant regulations and internal policies.
- Monitoring data access and usage, ensuring compliance with data privacy laws and the Data Protection Act, managing data access permissions.
- Identifying and resolving data-related issues, such as data inconsistencies or inaccuracies; addressing data quality problems, coordinating with IT for technical issues, and facilitating communication between business units and technical teams.
- Acting as a liaison between different departments and teams to ensure effective data management and governance.
- Facilitating meetings, communicating data governance objectives, and collaborating with Data Owners, IT, and other stakeholders.
- Providing training and support to data users to promote best practices in data management and usage.
- Managing the entire lifecycle of data from creation to archiving and deletion.
- Implementing data retention policies, managing data archives, and ensuring proper data disposal.

5.6.8 External Stakeholders

- **Development Partners:** Support data governance initiatives through funding, technicalassistance, and capacity-building efforts.
- **Private Sector:** Collaborates with the ministry to leverage data for innovative solutionsand services in agriculture.
- **Academic and Research Institutions:** Contribute to data governance through

research,analysis, and the development of new methodologies and tools.

Data Sharing Flow for External Stakeholders

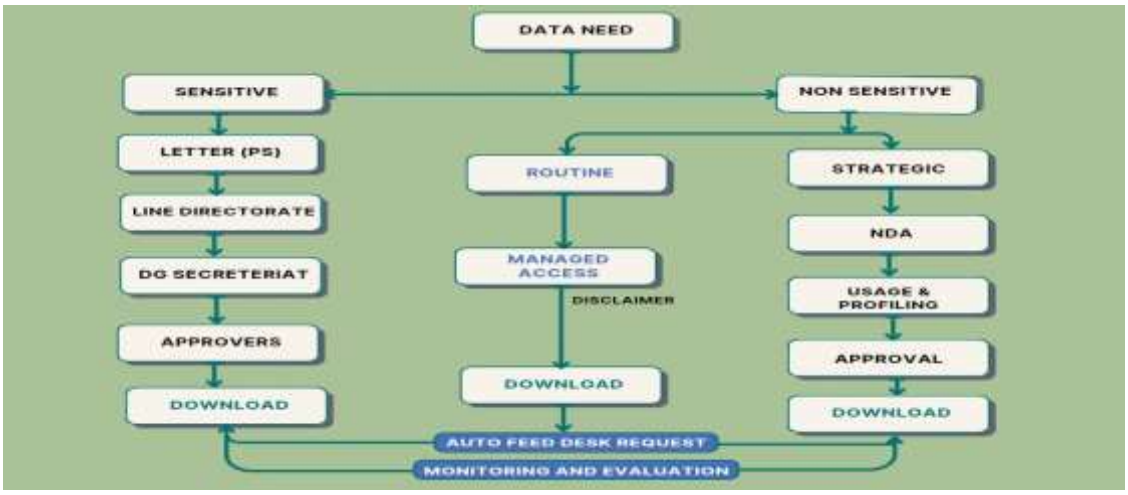


Figure 3Data Sharing Flow structure for External Stakeholders

Note: for the internal stakeholders they will use MOALD procedures and best practices already in place

5.7 Conclusion

The institutional framework within KAIMIS Data Governance Framework is designed to ensure effective management and utilization of agricultural sector data for enhancing agricultural productivity, ensuring food security, and promoting sustainable development in Kenya

5.4 Guidelines, Procedures, Tools & Training

5.4.1 Guidelines

Data governance guidelines (and policies) are essential in supporting the data governance framework within an organization. Policies define the principles, roles, responsibilities, and standards for data management to ensure data quality, security, and compliance with legal and regulatory requirements in areas such as: -

- **Data Quality and Integrity:** Standards for maintaining accurate, consistent data
- **Data Security and Privacy:** Measures to protect sensitive information from unauthorized access and breaches.
- **Data Access and Usage:** Rules governing who can access data, under what circumstances, and how it can be used.
- **Data Classification and Handling:** Procedures for categorizing data based on sensitivityand handling it accordingly.
- **Data Lifecycle Management:** Guidelines for data creation, storage, archiving, anddeletion to ensure proper data management throughout its lifecycle.
- **Compliance and Legal Requirements:** Ensuring data practices meet all relevant legal and regulatory obligations.
- **Roles and Responsibilities:** Defining the roles of data stewards, data owners, and other stakeholders in managing data.

5.4.2 Procedures

Clear procedures are vital in the document for ensuring consistent and efficient data management. They define standardized methods for data access, sharing, incident management, and data lifecycle management, which help maintain data integrity and security. By providing a clear framework for handling data, these procedures prevent misunderstandings, reduce errors, and enhance overall organizational efficiency in datagovernance.

The main procedures to be documented include:

- **Data Access Procedures:** Guidelines for who can access data and under what conditions.
- **Data Sharing Procedures:** Protocols for sharing data between departments or externalentities.
- **Incident Management Procedures:** Steps to be taken in case of data breaches or otherdata-related incidents.
- **Data Lifecycle Management Procedures:** Processes for managing data from creation todeletion, ensuring data quality and compliance throughout its lifecycle.

5.4.3 Tools

Utilizing appropriate tools for effective data governance enhances data security, and ensure compliance with regulations. These tools help organizations automate processes, maintain data integrity, and support decision-making, ultimately contributing to efficient and effective data governance and should be considered during the implementation of data governance framework. These categories can be explained as follows: -

- **Data Governance Platforms**: Comprehensive solutions that provide centralized management of data policies, roles, and processes.
- **Data Quality Management Tools**: Tools such as that help in profiling, cleansing, and monitoring data to ensure its accuracy and consistency.
- **Data Security Solutions**: Tools that protect data from breaches and unauthorized access by providing robust security measures and real-time monitoring.
- **Compliance Monitoring Systems**: for proper implementation the following tools that assist in tracking and ensuring adherence to regulatory requirements, conducting audits, and managing data privacy are required.

5.4.4 Agricultural Sector Data Gateway (ASDG)

- Data Repository: Serves as the central repository for agricultural data registries, providing aunified platform for data storage, data management, and managed access.
- Data Integration: Ensures seamless integration of data from various sources, enhancing data consistency and usability. This is a middleware for organizations to access KIAMIS data and allows for API integration for real-time data access and updates.
- User Access: The platform provides secure access to data for authorized users by stakeholder organizations and supports efficiency in decision-making processes across the agriculture sector.
- Data Privacy by design: The ASDG has incorporated data privacy standards in its design implementation including anonymization of personal data and security mechanisms to comply with data protection regulations

CHAPTER SIX:

Monitoring and Evaluation:

Provides the framework for evaluating the effectiveness of data governance initiatives, detailing objectives, indicators, and reporting mechanisms to ensure continuous improvement.

CHAPTER SIX: MONITORING AND EVALUATION

6.1 Introduction

The primary goal of M&E within KIAMIS Data Governance Framework is to ensure that the data governance processes are implemented effectively and yield the desired outcomes by tracking progress, evaluate the impact of data governance initiatives, and provide insights for continuous improvement. Key components of integral M&E system includes:

- **Performance Indicators**: The Secretariat at the National level and CASIMU will develop monitoring and Evaluation tools.
- **Regular Assessments**: Periodic assessments are conducted to evaluate progress and impact.
- **Reporting Mechanisms**: Regular reports are prepared and shared with all stakeholders to provide insights into performance and areas for improvement and coordination.

6.2 Key Components of the M&E Framework

6.2.1 Objectives and Indicators

- **Clear Objectives**: The framework sets specific objectives for data governance, such as improving data quality, enhancing data accessibility, and ensuring data security.
- **Performance Indicators**: These objectives are linked to measurable performance indicators. For example, data quality can be measured through the accuracy and completeness of farmer registration data, while data accessibility might be assessed by the number of stakeholders accessing the Data Platform

6.2.2 Data Collection and Management

- **Data Collection Tools**: The framework outlines various tools and methods for data collection, including surveys, audits, and automated data collection systems.
- **Data Management Systems**: Efficient data management systems are crucial for storing, processing, and analyzing the data collected. These systems ensure that data is handled securely and is readily available for M&E activities.

6.2.3 Stakeholder Engagement

- **Inclusive Approach**: Engaging all relevant stakeholders, including government agencies, private sector partners, and farmers, is essential for effective M&E.

  Stakeholders are involved in setting objectives, defining indicators, and interpreting M&E results.
- **Capacity Building**: Training and capacity-building programs are provided to stakeholders to enhance their understanding and skills in data governance and M&E practices.
- **Regular Meetings:** DGC and DGTC Meetings: Regular meetings are held to review progress, address challenges, and make strategic decisions. Stakeholder Forums: Periodic forums bring together all stakeholders to discuss developments, share experiences, and foster collaboration.
- **Communication Channels:** Reports and Dashboards: Regular reports and dashboards provide updates on key metrics and progress. Digital Platforms: Online platforms and tools facilitate real-time communication and collaboration among stakeholders.
- **Feedback Loops:** Continuous Improvement: Feedback from stakeholders is used to

continuously improve data governance practices and policies. Grievance Redressal: Mechanisms are in place to address grievances and resolve conflicts effectively.

6.2.4 Reporting and Feedback Mechanisms

- **Regular Reporting**: The framework mandates regular reporting of M&E findings to all stakeholders. These reports provide updates on progress, highlight achievements, and identify areas needing improvement.
- **Feedback Loops:** Feedback mechanisms are established to ensure that insights from M&E activities inform decision-making and lead to adjustments in data governance strategies.

6.2.5 Evaluation Processes

- **Impact Evaluation**: Evaluating the impact of data governance initiatives is a critical component. This will involve assessing the long-term effects of these initiatives on agricultural productivity, food security, and other key outcomes.
- **Process Evaluation**: In addition to impact evaluation, process evaluations will be conducted to examine the efficiency and effectiveness of data governance processes. This helps identify best practices and areas for improvement

6.3 Challenges and Mitigation Strategies

The M&E framework also acknowledges several challenges and proposes strategies to address them:

6.3.1 Data Quality Issues

Incomplete or inaccurate data can undermine M&E efforts. To mitigate this, the framework emphasizes the importance of robust data validation processes and regular data audits.

6.3.2 Capacity Building and Resource Mobilization

The framework underscores the importance of building the capacity of all stakeholders involved in data governance.

This includes:

- **Training Programs**: Regular training sessions will be conducted to enhance the skills and knowledge of data managers, stewards, and users.
- **Knowledge management and practices**: Workshops and seminars will provide platforms for knowledge sharing and learning from best practices.
- **Resource mobilization and sustainability**: Efforts are made to secure funding and technical assistance from Government as the priority supported by the development partners where in need. The framework suggests leveraging ministry budget as well as collaborations and partnerships with internal and external stakeholders funding to overcome resource constraints.

6.3.3 Stakeholder Resistance

Resistance from stakeholders can hinder M&E implementation. The framework advocates for transparent communication and demonstrating the value of M&E to gain stakeholder buy-in.

6.3.4 Recommendations for Effective M&E

- To ensure the effectiveness of the M&E framework, the following recommendations are provided:
- Develop a Detailed M&E Plan: A detailed M&E plan should be developed, outlining

specific activities, timelines, responsibilities, and resource requirements.

- Use Technology: Leveraging technology can enhance data collection, analysis, and reporting processes. The use of digital tools and platforms is encouraged.
- Continuous Improvement: M&E should be viewed as an ongoing process. Regular reviews and updates to the M&E framework are necessary to adapt to changing conditions and emerging challenges.
- Collaboration and Learning: Promoting collaboration and knowledge-sharing among stakeholders can lead to more effective M&E practices. Learning from other sectors and countries can also provide valuable insights.

6.3.5 Conclusion

The M&E framework within the MoALD Data Governance Framework is comprehensive and well-structured, aiming to ensure the successful implementation of data governance initiatives. By setting clear objectives, engaging stakeholders, and leveraging technology, the framework seeks to create a robust system for tracking progress and evaluating the impact of data governance efforts. Continuous improvement and collaboration are emphasized as key factors in achieving the desired outcomes and promoting sustainable data in Kenya.

6.4 Risk Management Tool for KIAMIS Data Governance Framework

Based on the MoALD Data Governance Framework, the following risk management tool has been developed to identify, assess, and mitigate risks associated with data governance within the Ministry of Agriculture and Livestock Development (MoALD).

- Risk Management Process, Risk Identification
- Risk Assessment, Risk Mitigation, Risk Monitoring and Review

6.4.1 Risk Identification

Identify potential risks that could impact data governance. This includes risks related to data quality, security, accessibility, compliance, and stakeholder engagement. Examples of Potential Risks:

- Data breaches or cyber-attacks
- Inaccurate or incomplete data
- Lack of stakeholder buy-in
- Insufficient resources (financial, technical, human)
- Non-compliance with regulations

6.4.2 Risk Assessment

Assess the identified risks based on their likelihood and impact. This helps prioritize risks and determine the level of attention they require.

Table 1: Showing Risk Assessment Matrix

Risk	Likelihood	Impact	Risk Level
Data breach	High	High	High
Inaccurate data	Medium	High	Medium
Lack of stakeholder buy-in	Medium	Medium	Medium
Insufficient resources	High	High	High

Non-compliance	low	High	Medium

6.4.3 Risk Mitigation

Develop strategies to mitigate the identified risks. This includes preventive measures, contingency plans, and actions to minimize the impact of risks if they occur.

Table 2: Showing Risk Mitigation Strategies

Risk	**Mitigation Strategy**
Data Breach	Implement robust cybersecurity measures, conduct regular security audits, and provide cybersecurity training.
Inaccurate data	Establish data validation processes, conduct regular data quality assessments, and train data stewards.
Lack of stakeholder buy-in	Engage stakeholders through regular communication, demonstrate the benefits of data governance, and involve them in decision-making.
Insufficient resources	Mobilize resources through partnerships and external funding, prioritize activities, and optimize resource allocation.
Non-compliance	Ensure regular compliance audits, provide training on regulations, and establish clear compliance policies.

6.4.4 Risk Monitoring and Review

Continuously monitor and review risks and the effectiveness of mitigation strategies. This ensures that new risks are identified and managed, and existing risks are effectively controlled.

Table 3: Showing Monitoring and Review Plan

Activity	**Frequency**	**Responsible Party**
Security audits	Quarterly	IT Department
Data Quality assessments	Biannually	Data Governance Secretariat
Stakeholder engagement Sessions	Monthly	Data Governance Secretariat
Resource Allocation Review	Annually	MoALD FinanceDepartment
Compliance audits	Annually	Compliance officer
Review of risk managementstrategies	Bianually	Data Governance Steering Committee

6.4.5 Conclusion

The risk management tool for the MoALD Data Governance Framework provides a structured approach to identifying, assessing, mitigating, and monitoring risks. By implementing this tool, the Ministry can enhance the resilience and effectiveness of its data governance initiatives, ensuring better data quality, security, and stakeholder engagement. This will ultimately support the Ministry's goals of improving agricultural productivity and sustainability.

LIST OF APPENDICES

APPENDIX A: MOALD PERSONAL DATA TYPES

MINISTRY OF AGRICULTURE AND LIVESTOCK DEVELOPMENT

Introduction

The ministry processes and stores the following categories of personal data, in line with its mandates and functions:

a. Identification Data

- **Examples**: Full name, National ID number, Tax Identification Number (PIN), Passport number, Contact details (phone numbers, emails).
- **Purpose**: For registration of farmers, livestock holders, and ministry personnel. Supports MoALD in identifying individuals for subsidy programs, farmer registration, and ensuring communication for service delivery.
- **Storage Location**: National databases, MoALD-operated systems such as the **Agriculture Sector Data Gateway (ASDG)**, secure cloud storage, county-based databases.

b. Demographic Data

- **Examples**: Age, gender, location (home addresses), marital status, nationality, educational qualifications.
- **Purpose**: Used in research, tracking service eligibility, rural farming programs, and agricultural development projects.
- **Storage Location**: Centralized and county-level databases; also in GIS (Geospatial Information Systems) when combined with spatial data.

c. Financial Data

- **Examples**: Bank account details, mobile payment data (e.g., Mpesa), salary information, farm income details.
- **Purpose**: Utilized for financial transactions related to subsidies, compensation schemes, and ministry-related financial aid distribution.
- **Storage Location**: MoALD financial systems, Treasury payment platforms, encrypted cloud storage solutions.

d. Health and Veterinary Data

- **Examples**: Livestock health records, veterinary interventions, disease tracking data, vaccination records.
- **Purpose**: To track disease outbreaks, manage animal health, and implement veterinary services.
- **Storage Location**: Kalro and Konza

e. Geospatial Data

- **Examples**: GPS coordinates of farms, land ownership, satellite imagery, maps, agricultural land use patterns.
- **Purpose**: For land use management, agricultural zoning, climate monitoring, and crop health assessment.
- **Storage Location**: GIS platforms, cloud data lakes, and satellite data storage systems.

f. Transaction and Logistical Data

- **Examples**: Purchase records (seeds, fertilizers), service usage data (e.g., farming advisory services), program participation records.
- **Purpose**: Tracks the distribution of services and goods to farmers, monitors program effectiveness, and ensures proper use of subsidies.
- **Storage Location**: MoALD's transactional systems, program databases.

2. Purpose of Data Collection and Processing

Each type of data serves a specific purpose tied to MoALD's activities:

- **Support for Decision-Making**: Data informs national agricultural policies, such as crop management, livestock care, and resource allocation.
- **Service Delivery**: Personal data ensures effective registration, input distribution (seeds, fertilizers), and farmer advisory services.
- **Research and Development**: Used for demographic and spatial analysis, climate resilience studies, and rural development initiatives.
- **Compliance with Legal Obligations**: Data collection aligns with **Kenya's Data Protection Act 2019**, ensuring transparency and accountability.
- **Public Safety and Animal Health**: Veterinary records help manage zoonotic disease outbreaks, livestock vaccinations, and health monitoring.

3. Data Storage Locations

The ministry employs a combination of **on-premise** and **cloud storage solutions**, ensuring compliance with **Kenyan Data Protection Act 2019** and secure handling of sensitive information. These include:

- **Centralized Systems**:
  - **Agriculture Sector Data Gateway (ASDG)**: A key platform for managing agricultural data, offering secure access and ensuring compliance.
  - **County Databases**: Serve as regional hubs for storing and processing data related to localized agricultural activities.
- **Cloud Storage**:
  - Used for large-scale geospatial and transaction data, cloud solutions are compliant with international security standards and encrypted to protect sensitive information.
- **On-Premises Data Centers**:
  - Located in ministry-owned data centers, storing critical government data with strict access controls to prevent unauthorized access.

4. Data Access, Security, and Governance

To ensure the security and privacy of personal data, MoALD has implemented robust governance practices:

- **Data Custodians**: These individuals or entities are responsible for maintaining the security and physical storage of the data.
- **Data Stewards**: Appointed to manage data quality, security, and usage, ensuring alignment with the Data Protection Act.
- **Data Governance Council**: Oversees the ministry's data strategy and ensures that policies are followed and enforced.

5. Legal and Compliance Considerations

MoALD's handling of personal data must comply with the **Data Protection Act 2019**, which mandates:

- **Transparency**: All stakeholders must be informed about how their data is collected and used.
- **Integrity and Confidentiality**: Measures are in place to ensure that data is not lost, misused, or accessed by unauthorized persons.
- **Purpose Limitation**: Data is processed only for specific, legitimate purposes outlined during collection.

APPENDIX B: DATA PROCESSING AGREEMENT (DPA)

MINISTRY OF AGRICULTURE AND LIVESTOCK DEVELOPMENT

Introduction

This Data Processing Agreement ("Agreement") is entered into as of [Date], by and between [Your Organization's Name] ("Controller") and [Third Party Processor's Name] ("Processor").

1. Purpose and Scope

1.1 The purpose of this Agreement is to ensure that MOALD personal data shared with the Processor is handled in compliance with applicable data protection laws and standards. 1.2 The scope of this Agreement covers all data processing activities carried out by the Processor on behalf of the Controller.

2. Definitions

- **Personal Data**: Any information relating to an identified or identifiable natural person.
- **Processing**: Any operation performed on Personal Data, such as collection, recording, organization, structuring, storage, adaptation, retrieval, consultation, use, disclosure, or destruction.
- **Data Subject**: The natural person to whom Personal Data relates.

3. Data Processing Obligations

3.1 The Processor shall process Personal Data only on documented instructions from the Controller. 3.2 The Processor shall ensure that any person acting under its authority who has access to Personal Data is committed to confidentiality.

4. Data Protection Measures

4.1 The Processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including but not limited to: - Encryption of Personal Data. - Ensuring ongoing confidentiality, integrity, availability, and resilience of processing systems. - Regular testing, assessing, and evaluating the effectiveness of technical and organizational measures. 4.2 The Processor agrees to assist the Controller in ensuring compliance with its obligations regarding data security, data breach notification, data protection impact assessments, and consulting with relevant data protection authorities.

5. Sub-processors

5.1 The Processor shall not engage any sub-processors without prior specific or general written authorization from the Controller. 5.2 In case of general written authorization, the Processor shall inform the Controller of any intended changes concerning the addition or replacement of other processors, thereby giving the Controller the opportunity to object to such changes.

6. Data Subject Rights

6.1 The Processor shall assist the Controller in responding to requests from Data Subjects exercising their rights under applicable data protection laws, including but not limited to the rights of access, rectification, erasure, restriction, portability, and objection.

7. Data Breach Notification

7.1 In the event of a Personal Data Breach, the Processor shall notify the Controller without undue delay and, where feasible, within 24 hours after becoming aware of the breach. 7.2 The Processor shall provide the Controller with sufficient information to allow the Controller to meet any obligations to report or inform Data Subjects of the Personal Data Breach.

8. Data Retention and Deletion

8.1 Upon termination of the Agreement, the Processor shall, at the Controller's choice, delete or return all Personal Data to the Controller and delete existing copies unless otherwise required by law.

9. Audits and Compliance

9.1 The Processor shall make available to the Controller all information necessary to demonstrate compliance with this Agreement and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller.

10. Liability and Indemnity

10.1 The Processor shall be liable for any breach of this Agreement and agrees to indemnify the Controller for any damages, losses, or expenses incurred as a result of such a breach.

11. Term and Termination

11.1 This Agreement shall remain in effect as long as the Processor processes Personal Data on behalf of the Controller. 11.2 Either party may terminate this Agreement for breach by the other party if the breach remains uncured for 30 days following notice of the breach.

12. Governing Law

12.1 This Agreement shall be governed by and construed in accordance with the laws of [Jurisdiction].

Signatures

[Controller's Name & Title]
Date: _____
[Processor's Name & Title]
Date: _____

APPENDIX C: KIAMIS NON-DISCLOSURE AGREEMENT

MINISTRY OF AGRICULTURE AND LIVESTOCK DEVELOPMENT

Annex……KIAMIS Non-Disclosure Agreement/ MOU Outline

[Logo organization A] [Logo organization B]

PREAMBLE

This MEMORANDUM of UNDERSTANDING (hereinafter referred to as "MOU" is made on dd/mm/yyyy between:

[Organization A] located on [street], [city], Kenya (hereinafter referred to as "A" which expression shall, where the context admits, include its successors and assigns) of the first part

AND [Organization B] located on [street], [city], Kenya

AND [Organization A] and [Organization B] are individually referred to herein as a "Party" and collectively as the "Parties",

RECITALS

WHEREAS [Organization A] [description of organization A + mission]

WHEREAS [Organization B] [description of organization B + mission]

WHEREAS [Organization A] and [Organization B] [description of joint goal]

WHEREAS, this MOU is based on principles of trust, equality, and mutual benefits; NOW, THEREFORE, the Parties have come to the following understanding:

OBJECTIVE

The objective of this MOU will be to establish a framework to facilitate cooperation between the two institutions on sharing of…… data

ARTICLES OF OBLIGATIONS

In order to collaborate effectively, the Parties agree to the following obligations:

ARTICLE 1: OBLIGATIONS OF A

A will facilitate B to access its content in agricultural and livestock sectors during

AND [Organization A] and [Organization B] are individually referred to herein as a "Party" and collectively as the "Parties",

RECITALS

WHEREAS [Organization A] [description of organization A + mission]

WHEREAS [Organization B] [description of organization B + mission]

WHEREAS [Organization A] and [Organization B] [description of joint goal]

WHEREAS, this MOU is based on principles of trust, equality, and mutual benefits; NOW, THEREFORE, the Parties have come to the following understanding:

OBJECTIVE

The objective of this MOU will be to establish a framework to facilitate cooperation between the two institutions on …

ARTICLES OF OBLIGATIONS

In order to collaborate effectively, the Parties agree to the following obligations:

ARTICLE 1: OBLIGATIONS OF A

A will facilitate B to access its content in agricultural and livestock sectors during the execution of specific Scope of Works (SOWs). While A will facilitate and support B in establishing collaboration with other A partners focusing on agricultural and livestock data and other relevant technology dissemination during the execution of specific Scope of Works (SOWs)

ARTICLE 2: OBLIGATIONS OF B

B will work within the established and/or agreed frameworks under A either directly or through other A partners. While B will identify opportunities for collaboration with A that will advance the Parties' shared interests.

ARTICLE 3: JOINT OBLIGATIONS

The Parties agree to:

Take all the necessary technical and organizational measures in the collection and sharing of farmers' personal data and be compliant with the Kenya Data Protection Act 2019

3.2 Other obligations…

ARTICLE 4: DURATION

This MOU shall become effective immediately upon signature by the appropriate authorized representatives of each of the two institutions and shall remain valid for a period of [months/years] subject to review and/or termination as may be necessary by either party. This MOU may be renewed by a mutually written agreement of the parties hereto, executed at least [months/years] prior to the expiration of the initial term.

ARTICLE 5: TERMINATION

Either Party may terminate the MOU at any time upon notice of its decision at least three (3) months in advance, without the right to any compensation for the other Party. If, at the moment of the unilateral termination, specific tasks are pending, they will continue until the end of the said specific task.

Upon termination, any gains or losses in the pursuance of the provisions of this MOU shall be shared on mutually agreed ratios; failing such agreement, the same shall be shared equally between the parties.

Termination of Cause: Each Party shall have the right to terminate this Agreement or any SOW immediately upon a written notice in the event (a) the other Party is in material breach of this Agreement or such SOW, and such breach is not cured within thirty (30) days after receipt of written notice of the breach, or (b) if the other Party makes a general assignment for the benefit of creditors, or files a voluntary petition in bankruptcy, or if an involuntary petition in bankruptcy or similar proceeding is filed against such other Party and is not dismissed within ninety (90) days.

Survival: Articles 6, 11, and 12 shall survive the termination of this Agreement for any reason, together with any accrued but unpaid payment obligations and any other provisions which by their plain meaning are intended to survive.

ARTICLE 6: CONFIDENTIALITY

During the course of this MOU, either party may acquire confidential information or trade secrets of the other. Confidential information of a party means all information of whatever description, whether in permanently recorded form or not, and whether or not belonging to a third party, which by its nature is confidential or which the party identifies as confidential to itself.

It does not include information that is:

Independently created or rightfully known by, or in the possession or control of, the other party and not subject to any obligation of confidentiality on the other party;

In the public domain (otherwise than as a result of a breach of this agreement);

Required to be disclosed by law; was or is independently developed by the Receiving Party without use or reference to any information obtained from the Disclosing, or any Party acting on behalf of the Disclosing

Party, as demonstrated by the Disclosing Party's written records.

The Parties, together with their representatives, agents, and personnel, shall keep confidential anything which the other designates as, or which might reasonably be expected to be, confidential, unless otherwise required by a competent authority.

ARTICLE 7: NON-EXCLUSIVITY

Unless otherwise agreed, this MOU is a non-exclusive agreement, and both Parties are free to carry out other projects of any nature whatsoever with third parties.

ARTICLE 8: GOVERNING LAW

The Parties agree that the laws of Kenya shall apply to this MOU.

ARTICLE 9: SETTLEMENT OF DISPUTES

9.1 Amicable Settlement

The parties undertake for themselves, their agents, and/or servants to observe all established rules and regulations and to make further rules and regulations to govern the use of facilities in the conduct of any or all of the functions of this MOU. The parties shall use their best efforts to amicably settle all disputes arising from or in connection with this MOU or interpretation hereof.

9.2 Right of Arbitration

Any dispute between the parties as to matters arising pursuant to this MOU which cannot be settled amicably within THIRTY (30) DAYS after receipt by one party of the other party's request for such amicable settlement may be submitted to an Arbitrator mutually agreed upon by the parties for a decision in accordance with the provisions of the Arbitration laws of Kenya.

ARTICLE 10: FORCE MAJEURE

Neither party shall be liable in damages or have the right to terminate this MOU, for any delay or default in performing hereunder, if such delay or default is caused by conditions beyond its control, including, but not limited to Acts of God, Government restrictions (including the denial or cancellation of any operational or other necessary licenses), wars, insurrections and/or any other cause beyond the reasonable control of the party whose performance is affected.

ARTICLE 11: INDEMNITY

The parties always agree to keep each other fully and properly indemnified against all damages to or losses of any of their respective facilities resulting from negligent acts of omission or commission of their respective agents and/or servants.

ARTICLE 12: INTELLECTUAL PROPERTY AND CO-AUTHORSHIP

A shall retain ownership of all intellectual property rights, title, and interest XX that is not subject to this Agreement. Organization's IP. The Parties acknowledge and agree that all rights in and to any Intellectual Property created or arising from the content creation and design other than the Intellectual Property described in 12.1 & 12.2 shall be owned jointly by the parties, and the revenue made from commercializing the co-created content shall be shared equally.

ARTICLE 13: RELATIONSHIP BETWEEN PARTIES

Nothing contained herein shall be construed as establishing a relationship of agent and principal or master and servant as between the parties. Each party shall have full control of its operations and undertakings and shall be responsible for activities and duties carried by and on its behalf.

ARTICLE 14: INSURANCE

In carrying out the functions of this MOU, each party will insure its own employees and ensure that all adequate safety precautions are in place.

ARTICLE 15: NOTICES

Any notification, request, or consent required or permitted to be given or made pursuant to this MOU shall

be in writing. Any such notification, request, or consent shall be deemed to have been given or made when delivered in person to the authorized representative at the Head Office of the party to whom the communication is addressed or when sent by registered mail, fax, or E-mail (signed attachments) to such party at the following address:

For: Head Office Representative, Organization A Contacts

For:

Head Office Representative, Organization B Contacts

PROVIDED THAT a party may change its address, e-mail, and fax number for communication hereunder by notifying the other party of such change pursuant to this clause. Notice shall be deemed to have been received one day after dispatch by electronic means and five days after dispatch by ordinary post.

ARTICLE 16: AUTHORIZED REPRESENTATIVE

Any action required or permitted to be taken, and any document required or permitted to be executed under this MOU may be taken or executed: on behalf of A by the [Head of Office representative] or any other Officer appointed in writing by the [Head of Office representative] to carry out that function on behalf of organization A. ORGANIZATION A ORGANIZATION B In witness thereof, the representatives of the agreeing Parties are duly authorized sign this MOU on the date indicated below:

By: _____	By: _____
(Signature)	(Signature)
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____
In the presence of (….)	In the presence of (….)
Signature: _____	Signature: _____
Name: _____	Name: _____
Date: _____	Date: _____

APPENDIX D: GUIDELINES FOR OFFICIAL DATA SHARING

MINISTRY OF AGRICULTURE AND LIVESTOCK DEVELOPMENT

Guidelines for Official Data Sharing

Based on the MoALD Data Governance Framework, the following guidelines outline the principles, procedures, and responsibilities for sharing data within the Ministry of Agriculture and Livestock Development (MoALD) and with external stakeholders.

Principles of Data Sharing

A. Sharing of open Data

In line with the Access to Information Act 2019, the MoALD shall avail Open data to thepublic as a social good. Open data refers to data that is freely available for anyone to access, use, and share. Open data aim to foster transparency, innovation, and collaboration by making data freely available for research, development, and decision- making processes

The key principles for sharing Open Data are:

1. Accessibility: The Open data shall be made easily accessible, through the Ministry website and other official channels. The data shall be made available in the most convenient and usable formats.
2. Licensing: The Open data shall be provided under the open license that permitsanyone to use, modify, and share the data without restrictions.
3. Machine-readable: The data shall be provided in a format that can be easily processed by a computer and other data analytics software.
4. Non-proprietary: The Open data shall not be tied to any proprietary software, ensuring that it can be accessed and used without the need for specialized, paid tools.
5. Comprehensive and Timely: Open data shall be as complete and up-to-date aspossible.

The MoALD policy statement on Open Data provides the legal basis for Open Data sharing.

B. SHARING OF PERSONAL DATA

Apart from the Open Data, the Ministry shall facilitate access and use of personal data while ensuring complete compliance with all the regulations under the Data Protection Act 2019. For the access of such data, the following Guidelines shall be applied:

1. Transparency: Data sharing processes shall be transparent, ensuring all stakeholders understand how data is shared and used.
2. Security: Shared data shall be protected against unauthorized access and breaches;
3. Compliance: Data sharing shall comply with relevant laws, regulations, and policies;
4. Quality: The shared data shall be accurate, complete, and reliable;
5. Accessibility: Data shall be easily accessible to authorized users while respecting privacy and confidentiality requirements;

6. Interoperability: Data systems shall be able to communicate and exchange data effectively.

Procedures for Sharing Personal Data

1. Request for Data Sharing

a) Internal Requests

Data users within State Departments, State Corporations, projects and programmes within MoALD can request for personal data by submitting a data request form to Data Governance Secretariat. In line with the regulation 21(6) of the Data Protection (General), the request shall be madein writing, and shall specify:

(a) the purpose for which personal data is required;

(b) the duration for which personal data shall be retained; and

(c) Proof of the safeguards put in place to secure personal data from unlawful disclosure.

b) External Requests

The external stakeholders including Counties, researchers, private sector, other partners, shallsubmit a formal data request also detailing the purpose, scope, and duration of data use.

2. Evaluation of Data Requests

- Assessment Criteria: Data requests shall be evaluated based on relevance, necessity, compliance with policies, and potential benefits.
- Approval Process: The Data Governance Technical Committee (DGTC) shall review and approve or decline the data requests. When an external request is declined, the DG Secretariatshall provide the reasons for the decline.

1. Data Sharing Agreements

- None Disclosure Agreement (NDA): An NDA shall be signed between MoALD and the requesting party, outlining the terms and conditions of data sharing.
- Elements of the Data Sharing Agreement: The signed data-sharing agreementshall specify:
- How the data can be used, including restrictions, data security measures, and confidentiality requirements.
- A description of the entities signing the agreement
- A statement summarizing the purpose of the agreement, i.e., what are theobjectives of data sharing
- The main contacts in each organization for queries about the data
- Any financial agreement that may cover how both costs and benefits aredistributed

Define what data will be shared

- Specify the name, description, and any unique reference number to identify thedata to be shared
- If the data is described in a data catalogue accessible to both parties, it might be described most easily and clearly by referencing its catalogue entry.
- Determine the structure (e.g., attributes, parameters, etc.) of data that to beshared
- Time period the data covers (if appropriate) & Format of data quality required
- Define the source of the data (one organization or from a combination of different sources (for the latter, intellectual property rights could have implications for how

the data can be shared and used))

- Information about whether the contributing sources know that the data will be shared
- Define if the sharing is a one-off transfer or if updates are to be made. If updates are required: Would they be as necessary corrections to the data? Would they be additions to the data? How regularly can they be made? If this is a one-off transfer of data, when will the data be provided?
- Clearly outline roles and responsibilities. Where possible, include name and contact details of organization representatives as well as a description of roles and responsibilities, e.g., who will prepare and update data, who will monitor implementation of the agreement, who to contact to resolve disputes, etc.

Determine how the data will be shared

- Modalities for sharing the data between the parties (e.g., among MoALD,KALRO, and Counties)
- Define where data is going to be stored & responsible for hosting the data
- Specify the security measures to be taken to secure sensitive data
- Determine how long the data is going to be shared for
- Define if data copies have to be destroyed at the end of the agreement and howthis will be verified

Specify how the data will be used

- Permissions needed for each party describing how they can use the data
- Requirements to follow & retain permissions, e.g. to attribute the source ofdata
- Restrictions that might be set to limit the use of the data, e.g., sharing data with third parties
- Define whether the data can be used in commercial products and services
- Consider whether permissions are needed (e.g., from third parties or individual consent) to share or use the data

2. Data Preparation and Transfer

- Data Anonymization: Personally identifiable information (PII) shall be removed ormasked to protect privacy.
- Data Format: Data shall be prepared in a standard format agreed upon by both parties.
- Secure Transfer: Data shall be transferred using secure methods (e.g., encrypted emails, secure file transfer protocols).

3. Monitoring and Compliance

- Usage Monitoring: Data usage shall be monitored to ensure compliance with theterms of the Data sharing agreement.
- Periodic Audits: Regular audits shall be conducted to verify that data sharing practices adhere to policies and agreements.

4. Requesting Parties

- Submit detailed data requests and adhere to the terms of data sharing agreements.
- Ensure data security and compliance with all applicable laws and policies.

Compliance and Legal Considerations

1. Regulatory Compliance:

- Data sharing shall comply with national laws such as the Data Protection Act and any other guidelines from the ODPC on data sharing.
- International data sharing shall comply with relevant international regulations and agreements.

2. Confidentiality and Privacy

- Data sharing agreements shall include clauses to protect confidentiality and privacy of individuals.
- Sensitive data shall be anonymized or de-identified to prevent unauthorized identification.

3. Intellectual Property Rights

- Respect and protect intellectual property rights associated with shared data.
- Ensure proper attribution and use of data as per the terms of the data sharing agreement.

Security Measures

1. Data Encryption

- Encrypt data during transfer and storage to prevent unauthorized access.
- Use strong encryption standards and regularly update encryption protocols.

2. Access Controls

- Implement role-based access controls to limit data access to authorized personnel.
- Regularly review and update access permissions.

3. Incident Response

- Develop and maintain an incident response plan to address data breaches or security incidents.
- Promptly report any data breaches to relevant authorities and stakeholders.

4. Review and Update of Guidelines

- The data-sharing guidelines should be reviewed and updated regularly to adapt to emerging challenges and changes in the regulatory environment.
- Feedback from stakeholders should be incorporated to continuously improve thedata-sharing processes.

APPENDIX E: PROCEDURE ON COMPLAINT HANDLING

MINISTRY OF AGRICULTURE AND LIVESTOCK DEVELOPMENT

STEP 1: All complaints/compliments about KIAMIS should be channeled to info@kilimo.go.ke for collation.

STEP2: All complaints/complements submitted orally to be recorded at the complaints register at the receptions of the Offices.

STEP2: All visitors with complaints shall be guided to fill the complaints form and submit to the complaints box.

STEP 2: If the complaint is simple, the receiving officer shall resolve the complaint immediately and update the register.

STEP 4: The Head of Communications shall collate all the complaints obtained from the website/physical forms submitted to the complaints box and forward them to the public complaints committee on a weekly basis.

STEP 3: The Public complaints committee shall review the complaints.

STEP 4: If the complaint is moderate or major it shall be escalated to the immediate supervisor for further investigations and resolution. If the complaint is not resolved it shall be forwarded to the Senior Management for further action and resolution.

STEP 4: Based on the review of the complaints, the Public Complaints committee shall draft a report which shall contain the following details as per the CAJ complaints handling reporting template:

i. Date the complaint was received
ii. Complaint channel
iii. Name of the complainant.
iv. Complaint issue, Action taken & Root cause
v. Corrective action taken to resolve the complaint
vi. Status - this should state if the complaint is:
    a. Resolved b. On-going c. New
    ix. Pending complaints from previous quarter (resolved, ongoing)

APPENDIX F: MOALD ACCESS CONTROL POLICY

MINISTRY OF AGRICULTURE AND LIVESTOCK DEVELOPMENT

1. Purpose

This Access Control Policy is established to define the procedures for controlling and limiting access to personal data within the Ministry of Agriculture and Livestock Development. The policy ensures that personal data is accessible only to authorized personnel, in line with data protection laws and standards.

2. Scope

This policy applies to all employees, contractors, third-party service providers, and any other individuals who have access to personal data processed by the Ministry. It encompasses all systems, networks, and devices that handle personal data.

3. Access Control Principles

- **Least Privilege**: Access rights will be restricted to the minimum necessary for users to perform their duties.
- **Need-to-Know**: Access to personal data will only be granted to individuals whose job responsibilities require it.
- **Role-Based Access Control (RBAC)**: Access privileges are assigned based on the individual's role within the Ministry. Each role is pre-defined with specific access rights aligned with job responsibilities.
- **Separation of Duties**: To reduce the risk of unauthorized access or modifications, critical tasks will be divided among multiple personnel.

4. Access Management Procedures

4.1 User Access Requests

- Access to personal data must be requested via an Access Request Form, approved by the immediate supervisor, and authorized by the IT Security Officer.
- Access requests will be reviewed by the Data Protection Officer (DPO) to ensure alignment with data protection principles.

4.2 User Access Levels

- **Administrator Access**: Granted to IT administrators and data managers responsible for managing access controls and system configurations.
- **Standard User Access**: Granted to employees based on their job roles, limiting access to personal data strictly necessary for their duties.
- **Temporary Access**: Granted to contractors or third-party service providers for a specified duration and scope. Temporary access will be deactivated upon task completion.

4.3 Access Authorization

- The IT department, in consultation with the DPO, will assign access privileges based on predefined role-based access levels.
- Changes in job responsibilities will be reviewed by the IT Security Officer to adjust or revoke access privileges accordingly.

5. Authentication and Password Management
5.1 User Authentication

- All users must authenticate using unique usernames and passwords.
- Multi-factor authentication (MFA) is required for access to systems containing sensitive or high-risk data.

5.2 Password Policy

- Passwords must be at least eight characters long and include a combination of letters, numbers, and special characters.
- Passwords must be changed every 90 days, and users are prohibited from reusing their previous five passwords.

6. Access Review and Monitoring
6.1 Periodic Access Reviews

- Access privileges will be reviewed every quarter to ensure that they are consistent with users' current roles and responsibilities.
- The IT Security Officer and DPO will conduct audits to ensure compliance with access control policies and document findings.

6.2 Access Revocation

- Access to personal data will be revoked immediately upon termination of employment, contract completion, or role changes that no longer require such access.
- The IT department will ensure that all access credentials, tokens, and keys are deactivated promptly.

7. Data Access Monitoring

- Access to systems containing personal data will be logged, capturing details of access attempts, including date, time, user identity, and access actions.
- Unusual or suspicious access activities will trigger alerts, which the IT Security Officer will review to determine appropriate actions.

8. Third-Party Access
8.1 Third-Party Access Agreements

- All third-party service providers with access to personal data must sign a Data Processing Agreement specifying access control and security requirements.
- Access provided to third parties will be limited in scope and duration and must align with the Ministry's data protection standards.

8.2 Third-Party Monitoring

- Activities of third-party service providers will be subject to regular monitoring, and any suspicious activities will be investigated and reported to the DPO.

9. User Responsibilities

- Users must not share access credentials with others and are required to report any suspected unauthorized access immediately to their supervisor or the IT Security Officer.
- Users must lock their devices when not in use and follow the Ministry's policies on data security and privacy.

10. Training and Awareness

- Regular training sessions on access control and data security protocols will be conducted for all employees and contractors.
- Employees must complete access control training annually and acknowledge their understanding and compliance with this policy.

11. Policy Review and Updates

- This Access Control Policy will be reviewed annually or as needed to adapt to changes in regulatory requirements or operational needs.
- Any updates to this policy will be communicated to all relevant personnel, and additional training will be provided to ensure compliance.

Acknowledgment and Agreement

All employees, contractors, and third-party service providers must sign an acknowledgment form confirming they have read, understood, and agree to comply with this Access Control Policy.

APPENDIX G: DATA PROTECTION POLICY

MINISTRY OF AGRICULTURE AND LIVESTOCK DEVELOPMENT

INTRODUCTION

The Ministry of Agriculture and Livestock Development (hereinafter referred to as "the Ministry," "we," or "us") is committed to protecting the privacy and security of personal data in compliance with the Constitution of Kenya, the Data Protection Act, 2019, and other relevant laws. The Ministry employs the **Kenya Integrated Agricultural Management Information System (KIAMIS)** as a key tool to collect and manage data related to agricultural services, beneficiaries, and stakeholders. This policy outlines how the Ministry collects, processes, stores, and protects personal data obtained through KIAMIS. We recognize that your personal data is valuable and part of your identity, and we commit to handling it responsibly and transparently. This policy explains the types of data we collect through KIAMIS, the purpose for its collection, and your rights regarding your personal data.

CONSENT TO COLLECT PERSONAL DATA

By engaging with the Ministry and using KIAMIS to access its services, you consent to the collection, processing, and storage of your personal data as outlined in this policy. The Ministry ensures that your data is collected lawfully, fairly, and transparently and is only used for the purposes for which it was collected.
You are encouraged to review this policy periodically, as it may be updated in line with legal or operational changes. Any updates will be communicated through our official channels, and it is your responsibility to stay informed of these changes.

TYPES OF DATA WE COLLECT

Through KIAMIS, we collect the following categories of personal data to effectively provide agricultural and livestock services:

- **Identification Data**: Official names, National Identification Card number, Passport number.
- **Contact Information**: Email address, telephone number, residential address, and postal address.
- **Agricultural Data**: Information related to land ownership, farm size, crop type, livestock, and production outputs.
- **Financial Data**: Information on payments related to agricultural subsidies, grants, or loans, including bank account details or mobile money numbers.
- **Demographic Data**: Age, gender, and other demographic information for planning and policy-making purposes.
- **Payment Data**: Payment methods used for any financial transactions linked to services provided by the Ministry, including mobile money, credit/debit card information, and billing addresses.

PURPOSE OF DATA COLLECTION

The data collected through KIAMIS is used to:

- Register farmers, livestock keepers, and other stakeholders to provide government services.
- Distribute subsidies, grants, and loans to beneficiaries efficiently.

- Facilitate agricultural research, policy development, and resource allocation.
- Monitor and improve the delivery of agricultural services and programs.
- Communicate with farmers and stakeholders regarding available services, projects, and updates.
- Verify the identity of individuals seeking services.
- Ensure compliance with statutory and regulatory requirements, particularly in the management of agricultural resources.

LEGAL BASIS FOR DATA COLLECTION

The Ministry will collect and process your personal data through KIAMIS based on one or more of the following lawful grounds:

- **Your consent**, given voluntarily when accessing services or enrolling in programs.
- **Performance of a public duty**, where the Ministry carries out tasks in the public interest related to agriculture and livestock management.
- **Compliance with legal obligations**, including laws related to agriculture, environmental management, and national statistics.
- **Execution of a contract** where the data is necessary to provide specific services requested by the data subject.

DATA SHARING AND DISCLOSURE

We may share your personal data collected via KIAMIS with the following entities:

1. **Government Ministries, Departments, and Agencies**: For the effective implementation of agricultural policies, subsidy programs, and to update government records.
2. **County Governments**: To coordinate agricultural programs at the county level and enhance service delivery.
3. **Third-party service providers**: Where necessary, we engage service providers to support the management of KIAMIS and associated services, ensuring data protection agreements are in place to safeguard your information.
4. **Legal authorities**: If required by law, we may disclose personal data to legal authorities in response to court orders, statutory obligations, or regulatory requirements.

We do not sell or rent personal data to third parties for marketing or any other commercial purposes.

DATA RETENTION

The Ministry will retain your personal data collected via KIAMIS only for as long as it is necessary for the purposes for which it was collected, or as required by law. Retention periods include:

- **General personal data**: Retained for the duration of the relevant agricultural program or service and up to five (5) years after service delivery for auditing and compliance purposes.
- **Payment data**: Retained for a minimum of seven (7) years to meet legal and tax obligations.
- **Agricultural and demographic data**: Retained indefinitely for research, policy development, and planning purposes, or until a lawful request for deletion is made.

DATA SECURITY

The Ministry takes appropriate measures to secure personal data collected via KIAMIS against unauthorized access, disclosure, alteration, or destruction. Our data security measures include:

- **Encryption**: Sensitive data is encrypted to protect it during transmission and storage.
- **Access control**: Access to personal data is restricted to authorized personnel only.
- **Regular security assessments**: We routinely test our security systems to ensure they meet the latest cybersecurity standards.
- **Data breach response protocols**: In the event of a data breach, affected individuals will be notified in accordance with the Data Protection Act, 2019, and any relevant regulations.

YOU'RE RIGHTS

As a data subject, you have the following rights under the Data Protection Act, 2019, regarding your personal data collected through KIAMIS:

- **Right to be informed**: To know how and why your data is collected and used.
- **Right of access**: To request access to the personal data held about you.
- **Right to rectification**: To correct inaccurate or incomplete data.
- **Right to erasure**: To request the deletion of your data in certain circumstances.
- **Right to restrict processing**: To limit how your data is used.
- **Right to data portability**: To request a copy of your data in a format that can be transferred to another entity.
- **Right to object**: To object to the processing of your personal data, particularly where it is used for research or statistical purposes.

To exercise any of these rights, please contact our Data Protection Officer (DPO) at: info@kilimo.go.ke

CORRECTION OR DELETION OF PERSONAL DATA

If you wish to correct or delete any personal data held by KIAMIS, you can submit a formal request to the Ministry's Data Protection Officer. Any requests to modify or delete personal data must comply with legal requirements, particularly where official government records are involved. Corrections may require identity verification, and deletion requests will be assessed based on the legal obligations for data retention.

CHANGES TO THIS POLICY

This Data Protection Policy may be updated periodically to reflect changes in law, technological advancements, or best practices in data protection. The latest version will be published on the Ministry's website. We encourage you to review the policy regularly to stay informed about how we protect your personal data.

CONTACT INFORMATION

For any questions, concerns, or to exercise your data protection rights, please contact:
Data Protection Processor/Controller
Ministry of Agriculture and Livestock Development
PO Box 30028-00100
Cathedral Road, Nairobi - Kenya
Email: info@kilimo.go.ke
Telephone: **+254-20-2718870**

APPENDIX H: ENCRYPTION/BACKUP POLICY

MINISTRY OF AGRICULTURE AND LIVESTOCK DEVELOPMENT

ENCRYPTION / BACKUP POLICIES

Encryption and backup policies are crucial in safeguarding MOALD personal data, particularly in systems, which handles sensitive agricultural and personal data.

1. Encryption Policy

Objective: Ensure that personal and sensitive data is encrypted both at rest and in transit to prevent unauthorized access.

- **Data at Rest Encryption**:
  - All personal data stored within KIAMIS should be encrypted using strong encryption standards such as **AES-256**.
  - Database systems, storage systems, and file systems should implement encryption at the storage level, ensuring that any extracted or archived data remains encrypted.
- **Data in Transit Encryption**:
  - Personal data transmitted between users and KIAMIS or between KIAMIS and other systems should be encrypted using **TLS (Transport Layer Security)** to prevent interception during transmission.
  - VPNs or secure communication channels should be used when data is transferred between different sites or databases.
- **Encryption Key Management**:
  - Secure, centralized encryption key management should be implemented.
  - The Ministry should use **Hardware Security Modules (HSMs)** or equivalent technologies for secure generation, storage, and rotation of encryption keys.
  - Ensure proper auditing of key usage to prevent unauthorized access to the keys.

2. Data Storage Policy

Objective: Implement secure storage practices to maintain data confidentiality, integrity, and availability.

- **Secure Storage Location**:
  - Personal data stored in KIAMIS should reside in secure data centers that adhere to international standards (such as **ISO/IEC 27001**).
  - Ensure that physical security controls are implemented, including restricted access to the data center and regular security audits.
- **Access Control**:
  - Enforce role-based access control (RBAC) within KIAMIS to ensure that only authorized personnel can access sensitive personal data.
  - Personal data should only be accessible to those with a legitimate need, and all access attempts should be logged and monitored.
- **Data Minimization**:

- Only the necessary personal data should be collected, and unnecessary or obsolete data should be securely deleted according to data retention policies.
- Ensure compliance with local data protection laws, such as the **Data Protection Act, 2019** in Kenya.

3. Backup Policy

Objective: Ensure that personal data in KIAMIS is regularly backed up and can be restored in the event of system failure or data corruption.

- **Regular Backups**:
  - KIAMIS data should be backed up regularly (e.g., daily or weekly), including full and incremental backups, to minimize data loss in the event of system failure.
  - Automated backup systems should be in place to ensure that all critical data is backed up as per schedule.
- **Offsite Backups**:
  - Personal data backups should be stored in **offsite locations** to mitigate the risk of data loss due to physical damage or cyberattacks at the primary data center.
  - Offsite backups should also be encrypted to protect data in case of unauthorized access.
- **Backup Retention Policy**:
  - Retain backups for a specified duration, depending on the legal and operational needs of the Ministry.
  - Ensure that older backups are securely deleted when no longer required.
- **Disaster Recovery**:
  - A disaster recovery plan should be implemented, ensuring that in the event of a data breach, system failure, or natural disaster, personal data can be restored from backups with minimal downtime.
  - Regular testing of backup restorations should be conducted to ensure system resilience and recovery effectiveness.

4. Data Integrity and Audit Trails

Objective: Ensure data accuracy and traceability of access or changes to personal data within KIAMIS.

- **Audit Trails**: Implement audit trails within KIAMIS to monitor access to personal data and track any modifications, deletions, or unauthorized attempts to access sensitive information. Logs should be maintained securely and reviewed regularly to detect any potential security breaches or policy violations.
- **Data Integrity**: Use cryptographic hash functions (e.g., **SHA-256**) to verify the integrity of personal data in storage and during transfers, ensuring that data has not been tampered with.

5. Compliance with Data Protection Laws

Objective: Adhere to legal requirements regarding personal data management, including encryption, storage, and backup.

- **Data Protection Act, 2019 (Kenya)**:
  - KIAMIS must comply with Kenya's Data Protection Act, 2019, which outlines the obligations for collecting, processing, storing, and sharing personal data.
  - Regular audits and assessments should be conducted to ensure compliance with data protection regulations.
  - Data subjects (e.g., farmers) should be informed about how their personal data is used and stored, and they should have the right to access, correct, or request deletion of their data.

APPENDIX I: VENDOR RISK MANAGEMENT (VRM) POLICY

MINISTRY OF AGRICULTURE AND LIVESTOCK DEVELOPMENT

Introduction

Vendor Risk Management (VRM) policies are critical for evaluating third-party vendors' data protection practices, particularly when dealing with sensitive systems. The Ministry of Agriculture and Livestock Development in Kenya, like other organizations handling personal data, should implement robust vendor risk management policies to ensure that third-party vendors comply with data protection standards.

Vendor Risk Management Policies and Procedures for Evaluating Data Protection Practices

1. Vendor Selection and Pre-Contract Evaluation

Objective: Ensure that all third-party vendors are thoroughly evaluated for their ability to protect personal data before engaging in any contract.

- **Vendor Data Protection Due Diligence**:
  - Conduct a comprehensive review of the vendor's data protection policies, focusing on encryption, access control, backup, and compliance with relevant laws such as **Kenya's Data Protection Act, 2019**.
  - Evaluate whether the vendor complies with international standards such as **ISO/IEC 27001** (Information Security Management) or **GDPR** (General Data Protection Regulation) if applicable.
- **Risk Assessment Questionnaire**:
  - Require the vendor to complete a risk assessment questionnaire that covers key areas such as:
    - Data encryption practices (in transit and at rest)
    - Data storage and backup protocols
    - Physical and network security measures
    - Access control policies and identity management
    - Incident response and breach notification procedures
- **Third-Party Audits and Certifications**:
  - Request the vendor to provide audit reports or certifications (e.g., **SOC 2 Type II** or **ISO/IEC 27001**) that demonstrate their adherence to high data security standards.
  - The Ministry should also perform independent audits or request access to third-party audit results to verify compliance.
- **Data Transfer and Storage Locations**:
  - Verify where the vendor stores and processes data. Ensure that personal data processed on behalf of KIAMIS is stored in secure data centers and that data transferred across borders adheres to Kenya's data protection laws and any other applicable regulations.

2. Vendor Contractual Obligations

Objective: Establish contractual obligations to ensure that third-party vendors adhere to strict data protection and security standards.

- **Data Processing Agreement (DPA)**:
  - Incorporate a **Data Processing Agreement (DPA)** into contracts, outlining how the vendor processes personal data on behalf of KIAMIS.
  - Specify the responsibilities of both parties, including the vendor's obligation to implement appropriate security measures, data retention policies, and breach notification requirements.
- **Confidentiality and Access Control**:
  - Ensure the contract stipulates that vendor employees must sign **Non-Disclosure Agreements (NDAs)** and are subject to background checks.
  - Limit access to KIAMIS data only to authorized personnel, and ensure that robust role-based access control mechanisms are in place.
- **Right to Audit**:
  - Include provisions in the contract that grant the Ministry of Agriculture and Livestock Development the right to audit the vendor's security practices, review their systems, and verify their adherence to the agreed-upon data protection standards.
  - Vendors should also be required to notify the Ministry of any changes in their security practices or infrastructure that may affect data protection.

3. Ongoing Vendor Monitoring

Objective: Continuously monitor and evaluate the vendor's data protection practices throughout the duration of the contract.

- **Regular Security Assessments**:
  - Conduct regular security assessments (e.g., annually or biannually) of the vendor's systems to ensure that data protection measures remain robust and aligned with the Ministry's policies.
  - Monitor the vendor's compliance with industry standards, and require them to undergo regular vulnerability assessments and penetration testing.
- **Risk Reassessment**:
  - Perform periodic risk reassessments based on factors such as new regulatory requirements, changes in the vendor's security posture, or updates to KIAMIS itself.
  - Vendors should also submit regular compliance reports detailing their adherence to data protection policies.
- **Incident Reporting and Response**:
  - Establish clear procedures for reporting data breaches or security incidents. Vendors must notify the Ministry immediately upon detecting a breach that affects KIAMIS data.
  - Ensure the vendor has a comprehensive **Incident Response Plan**, detailing steps for containing the breach, notifying affected parties, and preventing future incidents.

4. Data Encryption, Backup, and Retention Policies

Objective: Ensure that third-party vendors adopt strong data encryption, backup, and retention practices for KIAMIS data.

- **Data Encryption**:

  - Ensure that the vendor encrypts personal data at rest and in transit using industry-standard encryption algorithms such as **AES-256** or **TLS**.
  - Vendors must manage encryption keys securely, using centralized key management systems like **Hardware Security Modules (HSMs)**.
- **Data Backup**:
  - Verify that the vendor has regular, secure backup policies in place to protect against data loss. Backups should be encrypted and stored in geographically separate locations to ensure disaster recovery capabilities.
  - Vendors should conduct regular restoration tests to verify that backups are functional and data can be restored without corruption.
- **Data Retention and Deletion**:
  - Establish clear data retention and deletion policies in line with Kenya's Data Protection Act. Ensure the vendor securely deletes personal data when it is no longer needed for the agreed purposes.
  - Vendors should provide documented proof of secure data deletion or disposal of hardware containing KIAMIS data when applicable.

5. Compliance with Legal and Regulatory Standards

Objective: Ensure that vendors comply with all relevant legal and regulatory standards for data protection and privacy in Kenya.

- **Compliance with Kenya Data Protection Act, 2019**:
  - Vendors must comply with the **Kenya Data Protection Act, 2019**, which sets the legal framework for processing, sharing, and securing personal data.
  - Regular audits or reviews should be conducted to ensure vendors are adhering to local legal requirements and any updates to the legislation.
- **Cross-Border Data Transfers**:
  - If the vendor processes or stores data outside of Kenya, ensure that they comply with any restrictions on cross-border data transfers as stipulated by the Kenya Data Protection Act.
  - Ensure that any third-country transfers are governed by **Data Transfer Agreements** and meet the required data protection safeguards.

6. Vendor Off boarding and Data Disposal

Objective: Safely and securely terminate vendor relationships, ensuring that personal data is properly handled at the end of the contract.

- **Data Retrieval and Deletion**:
  - Upon termination of the contract, ensure that the vendor returns all personal data related to KIAMIS or securely deletes it from their systems.
  - The vendor should provide a **Certificate of Data Destruction** to confirm that all personal data has been permanently deleted.
- **Post-Contract Audit**:
  - Conduct a post-contract audit to verify that the vendor has adhered to all data protection policies, securely deleted data, and closed access to KIAMIS systems.
  - Retain documentation of the off boarding process and ensure that all access credentials are revoked to prevent any unauthorized access post-termination.

APPENDIX J: DATA RETENTION AND DELETION POLICIES

MINISTRY OF AGRICULTURE AND LIVESTOCK DEVELOPMENT

Introduction

Data Retention and Deletion Policies are critical for managing how long personal and agricultural data is retained and ensuring secure disposal when no longer needed. The following policies outline best practices for retaining and securely deleting data in line with legal and operational requirements.

1. Data Retention Policy

Objective: Ensure that data stored within KIAMIS is retained only for as long as necessary to fulfill legal, regulatory, and operational requirements, and that obsolete or redundant data is securely deleted.

- **Data Classification for Retention**:Data in KIAMIS should be classified based on sensitivity, purpose, and usage. Examples include:
  - **Personal Data**: Information about farmers, stakeholders, or employees.
  - **Agricultural Data**: Information on farm inputs, subsidies, or productivity.
  - **Transactional Data**: Data related to services, payments, or subsidies.

- **Retention Periods**:
  - **Personal Data**: Retain for the duration of the farmer's or stakeholder's active participation in Ministry programs, and up to a specific period after disengagement (e.g., **5 years**), depending on legal obligations.
  - **Financial and Transactional Data**: Retain for **7 years** to comply with Kenya's financial and auditing regulations.
  - **Agricultural Program Data**: Retain as long as necessary for reporting, auditing, and monitoring purposes, typically between **5 to 10 years**, depending on program timelines.
- **Compliance with Legal Framework**:
  - Ensure that all data retention complies with the **Kenya Data Protection Act, 2019**, which mandates that personal data should not be retained longer than is necessary for the purpose for which it was collected.
  - Retention periods must also comply with any other sector-specific regulations or international agreements Kenya has in place concerning agriculture, environmental, or financial data.
- **Data Access and Usage Monitoring**:
  - During the retention period, access to personal and sensitive data should be restricted to authorized personnel and monitored through role-based access control.
  - Conduct regular reviews of data usage and retention to ensure only relevant and necessary data is retained.

2. Archival Policy

Objective: Ensure that data which is no longer actively used but still within the retention period is securely archived for long-term storage.

- **Data Archival Process**:
  - Data that is no longer in active use (e.g., after a program's conclusion or completion of a transaction) should be securely archived.
  - Archived data should be stored in an encrypted and secure environment, with access limited to specific roles that require it for audit, regulatory, or reporting purposes.
- **Long-Term Storage**:
  - Archived data should be stored in locations with robust physical and digital security controls, ensuring protection against unauthorized access, corruption, or data loss.
  - Backup copies of archived data should be maintained to ensure recoverability in case of any storage failure.
- **Data Anonymization**:
  - For certain types of personal data, anonymization techniques can be applied to de-identify records, especially when the data is retained for statistical or research purposes.

3. Data Deletion Policy

Objective: Ensure the secure and permanent deletion of data once the retention period has expired, or the data is no longer required for legal or operational purposes.

- **Data Deletion Timeline**:
  - Once data reaches the end of its retention period, it must be securely deleted within a specified time frame, such as **90 days** from the retention expiry date.
  - For personal data, individuals whose data is stored should be notified when their data is deleted, in accordance with the KIAMIS data governance framework inline with Data Protection Act.
- **Secure Deletion Methods**:
  - **Personal Data**: Use secure data deletion methods (e.g., **data wiping** or **shredding**) to ensure that personal data cannot be recovered after deletion.
  - **Physical Media**: If personal data is stored on physical devices (e.g., hard drives or tapes), these should be physically destroyed or wiped using **degaussing** to ensure complete data eradication.
  - **Cloud Storage**: If KIAMIS data is stored in the cloud, deletion must comply with the cloud provider's data protection standards, ensuring that deleted data is completely wiped from all storage locations.
- **Data Deletion Verification**:
  - Maintain logs or certificates of data deletion for auditing purposes, providing evidence that data has been securely deleted.
  - Regular audits should be conducted to ensure that deletion procedures are being followed as per policy.

4. Exceptions to Deletion

Objective: Address situations where data must be retained beyond the standard retention period due to legal or operational requirements.

- **Legal Obligations**:
  - Data may need to be retained beyond its retention period to comply with legal investigations, court orders, or ongoing audits.
  - In such cases, data should be placed under a **legal hold**, preventing its deletion until the hold is lifted.
- **Operational Needs**:
  - Certain data may be retained for longer periods if required for ongoing research, agricultural studies, or national reporting.

- Where personal data is retained for these reasons, anonymization should be applied wherever possible to protect individual privacy.

5. Data Retention Compliance and Governance

Objective: Ensure the MOALD to be compliant with data retention and deletion policies through regular audits and governance mechanisms.

- **Governance and Oversight**:
  - Establish a **Data Governance Committee** to oversee data retention policies, ensuring compliance with regulatory frameworks and internal policies.
  - The committee should conduct regular audits of retention practices and review policies as necessary to accommodate changes in laws or operational needs.
  - **Audit Trails**:Implement audit trails for all data handling, including archiving and deletion activities, ensuring that all actions related to personal data are logged and can be reviewed if necessary. The audit trail should provide detailed records of data access, retention, archiving, and deletion actions to ensure full transparency.
  - **Employee Training**:Ensure that employees handling personal and sensitive data are trained in data retention and deletion policies, so they understand the importance of compliance and security in data management.

Key Elements of Data Retention and Deletion Policies

- **Retention Periods**: Data should be classified based on its sensitivity and purpose, with defined retention periods established for different types of data. Personal data might be retained for a specific number of years after the end of its active use, while transactional and operational data may have longer retention periods based on regulatory and operational requirements.
- **Archiving**:Data that is no longer actively used but still within its retention period should be securely archived. Archived data must be stored in an encrypted format with controlled access to ensure that it remains protected and accessible for future reference if needed.
- **Secure Deletion**:Once the retention period has expired, data must be securely deleted using methods that ensure it cannot be recovered. This includes data wiping, physical destruction of storage media, or following industry-standard deletion practices for electronic data.
- **Legal and Operational Holds**:In certain circumstances, data may need to be retained beyond the specified retention period due to legal requirements, investigations, or ongoing operational needs. Appropriate measures should be taken to place such data under a legal hold or ensure its anonymity when retaining it for research or reporting purposes.
- **Compliance Audits**: Regular audits should be conducted to verify compliance with data retention and deletion policies. Governance structures should be in place to oversee these practices, ensuring that they align with applicable laws and regulations.
- **Employee Training**: Personnel involved in data handling should receive training on data retention and deletion policies, emphasizing the importance of compliance, security, and privacy in data management.

APPENDIX K: MOALD DATA SHARING RECORD WITH THIRD PARTIES

MINISTRY OF AGRICULTURE AND LIVESTOCK DEVELOPMENT

Organization/Institution Name: [Insert]
Record Date: [Insert Date]
Data Protection Officer (DPO): [Name of DPO]
Prepared by: [Name of the person preparing the record]

1. Overview

This MOALD document records all instances of personal data sharing with third parties, outlining the purpose of the data sharing, the legal basis under the applicable data protection laws, and any relevant safeguards or agreements in place to protect the data being shared.

2. Data Sharing Summary Table

Third Party Name	Data Type Shared	Purpose of Sharing	Legal Basis	Date of Sharing	Data Retention Period	Security Measures	Third Party Country	Comments

3. Detailed Description for Each Data Sharing Instance

For more detailed records, you can include sections for each third party as shown below.

3.1 Third Party Name: [Insert Name]

- **Purpose of Sharing**: [Description of why the data is shared, e.g., etc.]
- **Data Type Shared**:[List the specific types of data shared, e.g., personal identification information, Farm records, etc.]
- **Legal Basis for Sharing**: [Consent, Contractual Necessity, Legal Obligation, Legitimate Interests, or Public Interest. Refer to specific provisions in the data governance framework in line with Kenya Data Protection Act or applicable laws.]
- **Data Retention Period**: [Specify how long the third party is permitted to retain the data, in line with the retention policies.]
- **Security Measures in Place**: [Describe MOALD security controls and protections applied to the data, such as encryption, anonymization, secure channels for transfer, or access control policies.]
- **Cross-Border Data Transfer**: [If applicable, describe whether the data is transferred outside of Kenya, and whether the receiving country provides adequate protection under applicable laws.]

- **Data Sharing Agreement**:[Mention if a Data Processing Agreement (DPA), Standard Contractual Clauses (SCCs), or Binding Corporate Rules (BCRs) are in place in MOALD to govern the data sharing.]

3.2 Third Party Name: [Insert Name]

- **Purpose of Sharing**: [Provide details.]
- **Data Type Shared**:[Provide details.]
- **Legal Basis for Sharing**: [Provide details.]
- **Data Retention Period**: [Provide details.]
- **Security Measures in Place**: [Provide details.]
- **Cross-Border Data Transfer**: [Provide details.]
- **Data Sharing Agreement**: [Provide details.]

4. Legal Basis for Data Sharing

4.1 Consent

- **Description**: When data subjects have provided explicit consent for their data to be shared with a third party.
- **Example**: Data shared for farming purposes where the subject has opted in.

4.2 Contractual Necessity

- **Description**: Data sharing is necessary for the performance of a contract with the data subject.
- **Example**: Sharing fertilizer distribution data with a farmer for processing.

4.3 Legal Obligation

- **Description**: Sharing data is required to comply with a legal obligation.
- **Example**: Providing personal data to tax authorities as part of legal requirements.

4.4 Legitimate Interests

- **Description**: Data sharing is necessary for the legitimate interests pursued by the organization or third party, provided these are not overridden by the rights of the data subject.
- **Example**: Sharing data with farming service provider to enhance system security.

4.5 Public Interest

- **Description**: Sharing data is necessary for tasks carried out in the public interest or for official functions.
- **Example**: Sharing data for farming purposes or government research.

5. Security Measures for Data Sharing

- **Encryption**: Personal data is encrypted before transmission to ensure secure sharing.
- **Access Control**: Only authorized individuals from the third party have access to shared data.
- **Data Anonymization**: When possible, data is anonymized or pseudonymized to reduce the risk of exposing identifiable information.
- **Data Transfer Channels**: Secure channels, such as VPNs or TLS, are used for transmitting data.

- **Third-Party Audits**: Third-party providers are regularly audited for compliance with data protection and security standards.

6. Cross-Border Data Transfers

6.1 Data Transfer Location

- Specify whether any data is transferred outside of Kenya, and if so, list the countries involved.

6.2 Adequacy of Data Protection

- Ensure that the receiving country offers adequate data protection measures, in line with the **Kenya Data Protection Act, 2019**, or use approved **Standard Contractual Clauses (SCCs)** or **Binding Corporate Rules (BCRs)**.

7. Conclusion

This document serves as a detailed record of all third-party data sharing, ensuring compliance with the Ministry of Agriculture and Livestock Development in line with the Kenya Data Protection Act 2019 and providing transparency in how data is handled, processed, and protected when shared with third parties.

Signed: _____
Date: [Insert Date]

APPENDIX L: INTERNATIONAL DATA TRANSFER INSTRUMENT FRAMEWORK

MINISTRY OF AGRICULTURE AND LIVESTOCK DEVELOPMENT

Date: [Insert Date]

1. Introduction

1.1 Purpose

- This document outlines the framework for managing international data transfers related to personal data processed within the Kenya Integrated Agriculture Management Information System (KIAMIS), ensuring compliance with Regulation 26 of the General Regulations under the Kenya Data Protection Act, 2019.

1.2 Scope

- This framework applies to all personal data processed in KIAMIS and outlines the procedures for evaluating and executing international data transfers.

2. Overview of Regulation 26

2.1 Data Localization Requirement

- Personal data must generally be stored and processed within Kenya unless specific conditions are met for international transfer.

2.2 Conditions for International Transfers

- Data may be transferred internationally if:
  - The data subject has consented to the transfer.
  - The receiving country provides adequate protection for personal data.
  - There are binding corporate rules or standard contractual clauses in place.
  - The transfer is necessary for the performance of a contract with the data subject.

3. Data Assessment for Localization

3.1 Data Classification

- Identify and classify the types of data collected, processed, and stored in KIAMIS, including:
  - Personal Data (e.g., farmer details, transaction data)
  - Non-Personal Data (e.g., agricultural statistics)

3.2 Data Localization Requirement: Ensure that all personal data is stored on servers located within Kenya, following applicable laws and regulations.

4. International Data Transfer Framework

4.1 Data Transfer Assessment

- Before initiating any international transfer, assess:
  - The legal framework of the receiving country.
  - The adequacy of data protection measures in place.

4.2 Consent Mechanism

- Develop clear procedures for obtaining explicit consent from data subjects for international data transfers, including:
  - Informing data subjects of potential risks.
  - Providing options for opting out.

4.3 Standard Contractual Clauses (SCCs)

- If transferring data to jurisdictions lacking adequate protection, implement SCCs to enforce data protection obligations on the receiving party.

5. Data Protection Impact Assessments (DPIAs)

5.1 Conduct DPIAs: Prior to any data transfer, perform a Data Protection Impact Assessment to identify risks and outline mitigation strategies.

6. Implementation of Adequate Safeguards

6.1 Technical and Organizational Measures

- Ensure that adequate safeguards are in place, including:
  - Data encryption during transfer.
  - Strict access controls to limit access to personal data.

6.2 Incident Response Plan

- Establish an incident response plan for data breaches that may occur during or after the transfer.

7. Compliance Monitoring

7.1 Ongoing Monitoring: Regularly monitor compliance with international data transfer policies and conduct periodic audits.

7.2 Training and Awareness: Provide training to personnel involved in data handling on international data transfer policies.

8. Conclusion

- The Ministry of Agriculture and Livestock Development is committed to ensuring compliance with data protection laws and safeguarding personal data during international transfers.

9. References

- Kenya Data Protection Act, 2019
- General Regulations under the Data Protection Act
- Relevant International Data Protection Standards

APPENDIX M: DATA SUBJECT CONSENT FORM

MINISTRY OF AGRICULTURE AND LIVESTOCK DEVELOPMENT

Introduction

This form provides information on how the Ministry of Agriculture and Livestock processes your personal data and outlines your rights. By signing this form, you consent to the processing of your personal data as described.

1. Data Controller MOALD

2. Purpose of Data Collection

MOALD personal data collected will be used for the following purposes:

- [Purpose 1, 2 ,3 ……N]

3. Types of Personal Data Collected

We will collect the following personal data:

- [Type of Data 1, 2, 3 ……N]

4. Legal Basis for Processing

The processing of your personal data is based on your consent, as per relevant data protection laws.

5. Data Sharing

Your data may be shared with the following third parties:

- [Third Party 1,2 ……..N]

6. Data Retention

Your data will be retained for [Retention Period] or as required by law.

7. Withdrawal of Consent

You have the right to withdraw your consent at any time. To withdraw consent, please contact [Contact Information]. Please note that withdrawing consent will not affect the lawfulness of processing based on consent before its withdrawal.

8. Data Subject Rights

As a data subject, you have the right to access, rectify, erase, restrict, and object to the processing of your data, as well as the right to data portability.

9. Declaration of Consent

By signing this form, you acknowledge that you have read and understood the terms of this consent and agree to the processing of your personal data as described.

Signature: _____

Date: _____

Printed Name: _____

10. Record of Withdrawal

If consent is withdrawn, record the date and reason for withdrawal here:

- Date of Withdrawal: _____
- Reason for Withdrawal: _____

APPENDIX N: ACCESS TO INFORMATION CONSENT FORM

MINISTRY OF AGRICULTURE AND LIVESTOCK DEVELOPMENT

APPLICANTS DETAILS

Name			
ID Number		Physical Address	
Mobile		Email Address	
Provide Summary of information being sought to be accessed & purpose:			

Type of access

- ❖ Internal ( )
- ❖ External ( )

For internal kindly follow the internal data access procedures and process and for external use specified procedure in line with KIAMIS data governance framework and ODPC regulations**.**

Methods of access preferred

- ❖ Original ( )
- ❖ Copies ( )
- ❖ Virtually ( )
- ❖ Others ( )

Explain your answer

……
……

SIGN:……. **DATE: …….**

Approved By: …….

SIGN:……. **DATE: …….**

APPENDIX O: COMPLAINTS FORM

MINISTRY OF AGRICULTURE AND LIVESTOCK DEVELOPMENT

NOTE: Information provided here will ONLY be used to process your complaint, and MOALD shall NOT share/disclose this information with a third party. We shall review and get back to you within 21 days. Kindly fold and drop in the complaints box at the reception. For further assistance, CONTACT US. Ministry of Agriculture and Livestock Development Cathedral Road, Nairobi P. O. Box 30028-00100 Kenya E-mail: info@kilimo.go.ke

Complaints Details (Information is voluntary….)

Name			
ID Number		**Physical Address**	
Mobile		**Email Address**	
Provide a brief description on your complaints			
Have you reported this matter to any public or private institutions related to the ministry? Yes No **If Yes Explain in details**			
Provide a summary of your complaints, and attach supporting documents if any (particulars of **what** happened, **where** it happened, **when** it happened and by **whom)**			
Suggest/Recommend possible actions to be taken:			
Was your complaint handled satisfactory by officers in charge? yes no explain in details			
Issue/Complaint Tracking Number: ……..			

Signature …… Date: ……..

APPENDIX P: FILE/LODGE COMPLAINT ON DATA SHARING & DISSEMINATION

Ministry of Agriculture and Livestock Development

Note

- Only use this form if you are a data subject, or acting on behalf of a data subject and filing a complaint in line with Section 56 of the Data Protection Act.
- If you have supporting documents to substantiate your claim, please annex copies to this form
- The information submitted will be treated with utmost confidentiality.
- If complaint is made on behalf of another data subject, please provide authorization to act on behalf of them.

A. PARTICULARS OF THE COMPLAINANT/REPRESENTATIVE

Name:
Phone number
Email Address
National ID / Passport Number

B. PARTICULARS OF THE RESPONDENT

Name (s) of the respondent (individual or institutional):
Name (s) and contact details of the respondent (individual or institutional):
Contact details of the respondent (individual or institutional):
Contact details of the respondent (individual or institutional):
Date of occurrence of the alleged infringement:

C. PARTICULARS OF THE COMPLAINT

Describe your complaint:
The name (s) of any persons that can provide further information relevant to the complaint, if any;
Any actual or potential harm or any urgency to be taken note of:

D. REMEDY SOUGHT

State in your view what redress/relief you are anticipating:
Which other steps have you already taken in relation to the complaint; if any
Particulars of any person or institution that has previously made attempts to resolve the matter:
In the event that the Respondent is contacted, do you wish to remain anonymous? Yes No
If so, please explain why?
Provide supporting documents that will assist in addressing this compliant. (For multiple documents, ensure to have all of them in a common folder)

APPENDIX Q: DATA BREACH REPORTING

Ministry of Agriculture and Livestock Development

Note: Only use this form if you are, or acting on behalf of, a data controller or data processor reporting a data breach in line with Section 43 of the Data Protection Act.

File a Complaint

Details of Controller/ Processor

Organization/Institution Name:

Contact Person Name:

Contact Number

Mobile No. Email Address

Other Contact Details:

Details of the Breach

Description of Data Breach:

Categories of persons affected by the data breach (e.g. farmer, customers, patients, employees, clients, children, vulnerable groups; etc.)

In addition, please select any categories that apply:

Financial Data

Additional details of the type of personal information involved in the data breach

Provide a detailed description of any action, including remedial action, you are taking, or intend to take to assist data subjects whose personal data was involved in the data breach.

(a) Short-term Measures (Immediate Actions):

Outline the immediate steps taken to secure the data and limit any potential damage.

(b) Medium-term Measures (System Improvements):

Detail the actions planned or in progress to strengthen data security systems.

(c) Long-term Measures (Policy and Training):

Describe the strategies for enhancing organizational data protection policies, including staff training programs on data security, updating incident response plans, and regular compliance reviews.

Provide detailed description of any action you have taken, or are intending to take, to prevent reoccurrence

Section: Communication with Data Subjects

Has the entity communicated with the data subjects affected by the breach? Yes No

If yes, please attach a sample of the communication sent to data subjects

If no, please provide a detailed explanation as to why communication has not occurred.

Specify the steps your organization/ agency recommends that individuals take to reduce the risk that they experience serious harm as a result of this data breach

Other entities affected: (if the data breach described above was also a data breach of another organization, provide their identity and contact details)

Date the breach occurred: (provide your best estimate if the exact date is not known):

Was Data Breach reported within 72 hours of Discovery? Yes No

If No, please specify why:
Date the breach was discovered (provide your best estimate if the exact date is not known)
Primary cause of breach:
Malicious or criminal attack
If other, please specify.

Description of how the data breach occurred
Number of data subjects whose personal data is involved in the data breach: 1-10
Exact number of data subjects whose personal data is involved in the breach (please provide your best estimate):
Is there any other information you wish to provide at this stage, or any matters that you wish to draw to the MOALD attention?
List of any other data protection authorities, law enforcement bodies or regulatory bodies that you have reported, or intend to report, this data breach to:
Attach Copy of Report to Other Regulator or Institution: such as police or data protection authorities.

Request for Confidentiality
I request that the particulars of the breach, mitigation efforts and responses, and additional information provided in this form be held by MOALD in confidence
If you request any information in this form be held by MOALD in confidence, please provide further information to support the request. MOALD will respect the confidence of commercially or operationally sensitive information provided voluntarily in support of a data breach notification, and will only disclose this information after consulting with you, and with your agreement or where required by law.

Attachments
Please attach any relevant documents that support your notification and actions regarding the data breach. This can include but is not limited to: (a) Sample Agreements (b) Incident Response Policy

Additional Provisions
Attach Incident Report: A section for uploading a detailed incident report.

Declaration:
I hereby declare that the information given in this application is true and correct to the best of my knowledge and belief

Review and Submit:
Please review the information that you have provided about the data breach. If you would like to change anything, you can return to the relevant section and update.

APPENDIX R: DATA ARCHIVING, RETENTION GUIDELINES

Ministry of Agriculture & Livestock Development

Preamble

The Ministry of Agriculture and Livestock Development (MoALD) and counties shall ensure that only data necessary for informed decisions and policies on relevant farmers' support services as well as effective implementation of national and county government mandates are kept. The need to retain data varies widely with the type of data and the purpose for which it was collected. The MoALD shall strive to ensure that data is only retained for the period necessary in line with the existing public information archiving and disposal laws and regulations.

Scope

This policy statement covers all data collected by the MoALD and stored on the owned data centers or backup systems & media, regardless of location. It applies to both data collected and held electronically (including photographs, video, and audio recordings) data that is collected & held as hard copy or paper files.

Data Classification

To determine whether data should be kept or not, the KIAMIS Secretariat shall classify data on its sensitivity, value, and regulatory requirements using the following criteria:

- **Open Data:** Data that can be freely shared with the public without any risk of harm or legal repercussions.
- **Internal Data:** Data intended for internal use only and not for public distribution such as internal memos, organizational charts, and internal project documents, etc
- **Confidential data**: Data that, if disclosed, could cause harm to the Ministry, counties or individuals, or data that could result into farmers' business losses if shared with other countries. The confidential data include farmers' registration data, business plans, detailed commodity export data, proprietary research, employee records, etc. Such data shall have access is limited to authorized personnel only.
- **Highly Confidential data:** Data that, if disclosed to any third party, could cause severe harm to the Ministry and Counties including trade secrets, financial data, and personally identifiable information. Such data shall be subject to the highest level of protection.
- **Data subject to regulatory compliance:** Data subject to specific regulatory requirements shall be identified and handled in accordance with the relevant regulations.
- **Contractual data:** Data subject to contractual obligations, including data shared with third parties under non-disclosure agreements (NDAs).
- **Data Lifecycle Stages:** the data shall be categorized into active data that is used for ongoing operations; archived that is no longer actively used but retained for legal, regulatory, or historical purposes; and disposable data that is subject to secure destruction following its relevant retention period.

Reasons for Data Retention

The MoALD shall retain only that data that is necessary to effectively conduct its program activities, fulfill its mission and comply with applicable laws and regulations. Reasons for data retention include:

- Providing an ongoing service to the data subject (e.g. sending a newsletter, publication or ongoing

program updates to an individual, ongoing training or participation in the MoALD's programs, processing of employee payroll and other benefits)

- Compliance with applicable laws and regulations associated with financial and programmatic reporting by the MoALD to its funding agencies and other donors
- Compliance with applicable labor, tax and immigration laws
- Other regulatory requirements and Security incident or other investigation
- Intellectual property preservation and Litigation

Data Duplication

The MoALD seeks to avoid duplication in data storage whenever possible, though there may be instances in which for programmatic or other business reasons data must be held in more than one place. This policy applies to all data in the MoALD's possession, including duplicate copies of data.

Retention Requirements

The MoA:LD has set the following guidelines for retaining all personal data in line with the Data Protection Act:

- The farmers' personal data shall be retained or sent to the national archives for potential use for the period the farmer is still alive but not more than one year if the farmer ceases to be practicing farming;
- Website visitor data shall be retained as long as necessary to provide the service requested/initiated through the MoALD website.
- Projects or programmes contributor data shall be retained for the years in which the individual projects are contributing and then for 3 years after the date of the last contribution.
- Projects and meeting participants personal data (including sign in sheets) shall be retained for the duration of the project that financed the program plus any additional time required under the terms of the project or grant agreement.
- Personal data of guarantees, subcontractors and vendors shall be kept for the duration of the contract or agreement.
- Employee data shall be held for the duration of employment and then 10 years after the last day of employment.

Data Destruction

Data destruction shall be taken to ensure that MoALD manages the data it controls and processes in an efficient and responsible manner. When destroying public data, the MoALD will be guided by the Public Archives and Documentation Service Act 2015 as well as the ICTA Electronic Records Management Standards, 2019. When the retention period for a particular data category expires, the MoALD shall send the datasets to the Director Kenya National Archives and Documentation Service for retention in line with the Public Archives and Documentation Service Act 2015. If data fall under destruction and not archiving category, the Ministry and counties shall follow the following steps leading to disposal of such data:

- Inventory and Classification: The KAIMIS Secretariat shall conduct a thorough inventory of data assets and classify the data to determine its sensitivity and retention requirements. Data subject to destruction include datasets of farmers who have passed on or have left farming; data for promotion of crops that are no longer scheduled, eg Tobacco; data on outdated technologies, etc
- Authorization and Approval: The KIAMIS Secretariat shall secure necessary approvals from Cabinet Secretary (data owners) or the Data Protection officer before proceeding with data disposal.

- Documentation of the Authorization: The KIAMIS secretariat shall maintain records of the destruction approvals for audit and compliance purposes.
- Selection of Appropriate Disposal Method: The KIAMIS secretariat shall choose the right disposal methods. including: physical destruction, shredding, incineration, or pulverizing physical media (e.g., paper documents, CDs, hard drives); Electronic Data Destruction: Using software tools to overwrite or wipe data on digital storage devices (e.g., hard drives, SSDs, USB drives); Degaussing methods such as using a degausser to disrupt the magnetic fields on magnetic media, rendering the data irretrievable; Destroying encryption keys to make encrypted data inaccessible, among other methods.

Before any data disposal, the KIAMIS Secretariat shall undertake Data Backup and Verification to ensure that no critical data is inadvertently deleted by verifying that all necessary backups and archives are in place.

Review and Auditing:

KIAMIS Secretariat shall record all steps taken during data disposal process, including dates, methods used, personnel involved, and verification results. Further, the Secretariat shall conduct regular audits of data disposal practices to ensure compliance with policies and regulations. This policy statement shall be subject to regular review and update in order to adapt to new threats, technologies, and regulations. The MoALD shall conduct periodic audits to ensure compliance with the policy and identify areas for improvement.

APPENDIX S: GUIDELINES FOR CROSS-BORDER DATE SHARING

MINISTRY OF AGRICULTURE AND LIVESTOCK DEVELOPMENT

1. The Ministry of Agriculture and Livestock Development strictly follows the Dat Protection Act 2019 when collecting and sharing any kind of personal data. In line with the Regulations 26 of the Act, the Ministry has developed clear guidelines for sharing personal data with third party international (cross-border) jurisdictions. When sharing any personal data across the borders, the Ministry legal team and KIAMIS data sharing designated officials are required to strictly follow these guidelines.

2. When handling cross-border data sharing, the Ministry legal team, KIAMIS Data Protection Officers and other authorized persons will seek support from Supervisory Authorities including Office of Data Protection Commission, department of foreign affairs and international trade, the office of Attorney General, among others, to asses, analyse and document all the relevant legal and regulatory frameworks on personal data sharing of the receiving countries/jurisdictions and alignment with the Kenya Data Protection Act 2019.

3. The multi-agency legal team working with the Ministry and KIAMIS officials will strive to understand, evaluate and document the implications of transferring data across borders, including potential legal restrictions or requirements and provide plans for relevant safeguards necessary for specific countries or regions. While developing the safeguard plans, the multi-agency team will take into account the existing regional and international trade agreements and regulations, country-to-country MoUs, as well as the cross-country cultural differences in attitudes toward privacy and data sharing. The team will also look into the financial, geo-political and ethical implications of sharing or not sharing personal data and strive for transparency, cooperation, dialogue and build trust among parties involved in data sharing.

4. Where personal data sharing involves different countries or regions, the Ministry legal team and KIAMIS officials will check the details of Standard Contractual Clauses (SCCs) and pre-approved contractual terms provided by regulatory authorities of the different jurisdictions (such as the European Union Deforestation Regulations (EUDR) provided by the European Commission), the General Data Protection Regulations (GDPR) of the foreign countries/regions and any other legal instruments required to facilitate the lawful transfer of personal data from Kenya to such external jurisdictions. Moreover, the legal team will check and confirm whether the cross-border data transfers are between two separate cross-border data controllers; or if transfers involve a data controller to a data processor; or if it is between two data processors. In any of the scenarios, the legal team will define the most relevant legal and regulatory requirements.

5. Where personal data sharing involves corporate entities of different countries (such as private Coffee Trading agencies in Kenya and those in Europe) the Ministry legal team and KIAMIS officials will examine the existing Binding Corporate Rules (BCRs) and other internal policies adopted by multinational organizations to facilitate cross-border personal data transfers; how such corporate BCRs align with the SCCs and the GDPR of the respective countries/regions of origin, and the relevant regulations under the Kenya Data Protection Act 2019.

6. Whether the cross-border personal data sharing is between nations, regions, or private corporations, the legal team and KIAMIS officials will strive to ensure that the SCCs, the BCRs and the GDPR of the external countries/ regions/ corporations are aligned with the Kenya Data Protection regulations, and the basic details including lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality, among others.

7. When handling cross-border data sharing, the KIAMIS officials will classify the data being shared based on the data sensitivity and special categories, and apply relevant safeguards measures such as data anonymization or pseudonymization; third party None Disclosure Agreements (NDAs), and other means that can be used to mitigate personal data sharing risks. The team will also determine if data owners' consent and rights such as own data access, rectification, or erasure, are necessary for the transfer of personal data and ensure that such consent, if required, are obtained efficiently and appropriately and the critical data subjects' rights are adhered to.

8. To ensure transparency and stakeholders' awareness about data cross-border personal data sharing and the relevant legal and regulatory frameworks, the Ministry will make available and accessible the relevant SCCs, BCRs and the GDPR of the foreign countries/regional blocks as well as relevant multinational corporations.

9. To institutionalize cross-border personal data transfers compliance, the Ministry will liaise with relevant institutions to undertake training and awareness creation amongst the government official, private corporations and key stakeholders involved in cross-border personal data exchanges.

10. The Ministry will establish mechanisms for routine monitoring and auditing of the established cross-border data sharing safeguards and undertake regular risk assessments of the established safeguards, so as to inform the implementation of strong security measures for data in transit and at rest, including encryption, access controls, NDAs and other relevant legal instruments.

11. Furthermore, the Ministry will regularly review and update the external personal data sharing protocols so as to reflect changes in laws, practices, or organizational structures and adjust the cross-country personal data sharing guidelines in response to evolving regional and global changes in the legal and regulatory requirements.

12. To ensure enforcement and redress complaints/disputes that may arise, the Ministry will liaise with the multi-agency team to create procedures and clear processes for handling disputes and grievances related to cross-border data processing and transfers, protocols for data breach notification and incident response, as well as means to ensure that data subjects can seek redress in the event of non-compliance, including liability clauses for non-compliance, arbitration and mediation clauses, efficient conflicts resolutions as well as the mechanisms for compensation to affected individuals. The clauses will also include provisions for the termination of the cross-border data sharing agreements.

APPENDIX T: AUDIT LOG FORMAT FOR TRACKING ACCESS AND CHANGES TO PERSONAL DATA

Ministry of Agriculture & Livestock Development

System: Kenya Integrated Agriculture Management Information System (KIAMIS)
Organization: Ministry of Agriculture and Livestock Development
Date: [Insert Date]
Prepared by: [Name of the person responsible for the log]

1. Purpose of the Audit Log

The purpose of this audit log is to track all instances of access to and changes made to personal data within KIAMIS. This ensures transparency, accountability, and compliance with data protection regulations. The audit log captures details of who accessed or modified personal data, the nature of the change, and the date and time of the activity.

2. Key Elements Tracked in the Audit Log

The audit log tracks the following key elements related to personal data access and changes:

- Date and Time of Access/Modification
- User ID/Employee Name (Who Accessed or Modified Data)
- Role of User
- Data Accessed/Modified (Type of Data)
- Action Performed (Accessed, Modified, Deleted, Exported)
- Description of Change (If Modified)
- IP Address or Device Used for Access
- Location of Access
- Reason for Access/Modification (If Applicable)
- Outcome (Success or Failure)
- Comments/Notes

Date & Time	User ID/Name	Role	Action	Data Accessed/Modified	Description of Change	IP Address/ Device	Location	Reason for Access	Outcome	Comments

4. Detailed Entry for Each Access or Modification

For more significant changes or access to critical data, additional details may be provided.

4.1 Example Entry

- **Date and Time**: 2024-10-07, 10:15 AM
- **User ID/Name**: John *****
- **Role**: System Administrator
- **Action**: Accessed Farmer Registration Data
- **Data Accessed**: Farmer personal information, including name, ID, and location details.
- **Description of Change**: No changes made; data accessed for review purposes.

- **IP Address/Device**: 192.168.1.1 / Desktop Computer
- **Location**: Nairobi Office
- **Reason for Access**: Data audit required by senior management.
- **Outcome**: Success
- **Comments**: Approved by supervisor; access logged for audit.

4.2 Example Modification Entry

- **Date and Time**: 2024-10-05, 3:30 PM
- **User ID/Name**: Jane *****
- **Role**: Data Officer
- **Action**: Modified Farmer Payment Information
- **Data Modified**: Updated bank account details for farmer ID #12345.
- **Description of Change**: Changed bank account number for farmer's subsidy payments.
- **IP Address/Device**: 192.168.2.3 / Laptop
- **Location**: Eldoret
- **Reason for Access**: Correction of farmer payment details based on new submission.
- **Outcome**: Success
- **Comments**: Farmer notified of changes, and confirmation email sent.

5. Retention of Audit Logs

5.1 Retention Period: Audit logs will be retained for a period of **5 years**, as per data protection requirements and internal retention policies. After this period, logs will be securely archived or deleted, unless a legal obligation requires extended retention.

5.2 Log Integrity: Logs will be protected from unauthorized access or modification by implementing strict access controls. Only authorized personnel, such as system administrators and compliance officers, can view or alter audit logs.

6. Compliance with Kenya Data Protection Act

6.1 Purpose of Logs

- These logs are maintained to comply with the **Kenya Data Protection Act, 2019**, ensuring that all access to and modifications of personal data are traceable, and that individuals' privacy is protected.

6.2 Regular Review

- Logs will be reviewed regularly by the **Data Protection Officer (DPO)** to identify any unauthorized access, suspicious activity, or security breaches.
- In case of any identified breach or anomaly, the organization will notify affected individuals and the **Office of the Data Protection Commissioner** as required by law.

7. Security Measures for Logs

- **Encryption**: All logs are encrypted during storage to prevent unauthorized access.
- **Access Control**: Only designated personnel with appropriate permissions can access or view logs.
- **Backup**: Logs are backed up daily to ensure data is not lost in case of system failure or compromise.

8. Conclusion

The audit logs maintained for KIAMIS are a critical component of the Ministry's data protection framework. By monitoring all access and modifications to personal data, the Ministry ensures that personal data is handled in accordance with legal requirements, and that the integrity and confidentiality of data are preserved.

Signed: _____

Date: [Insert Date]

APPENDIX T: DATA BREACH LOG

MINISTRY OF AGRICULTURE & LIVESTOCK DEVELOPMENT

Introduction

This Data Breach Log is maintained by the Ministry of Agriculture and Livestock Development, Kenya, to record all data breaches, providing details on the nature of each breach, the response actions taken, and follow-up steps. The log supports compliance with legal obligations and assists in improving data protection practices over time.

Data Breach Log Entry Template

For each data breach incident, fill in the details as follows:

Incident ID	Date of Breach	Date Reported	Breach Type	Data Compromised	Breach Description	Affected Individuals/Departments	Detection Method	Initial Containment Actions	Eradication Actions	Recovery Actions	Notifications Sent	Follow-Up Actions	Status	Review Date

Description of Data Breach Log Fields

- **Incident ID**: A unique identifier assigned to each data breach incident.
- **Date of Breach**: The date on which the data breach was detected or occurred.
- **Date Reported**: The date on which the breach was reported to the Incident Response Team.
- **Breach Type**: The type of breach, such as unauthorized access, data leakage, or ransomware attack.
- **Data Compromised**: A description of the type of data involved, such as personal or financial data.
- **Breach Description**: A brief summary of how the breach occurred, including any details known about the cause.
- **Affected Individuals/Departments**: A list of individuals or departments affected by the breach.
- **Detection Method**: How the breach was identified, such as through monitoring tools, reports from farmers, or alerts.
- **Initial Containment Actions**: Steps taken immediately to limit the impact of the breach, such as isolating affected systems or accounts.
- **Eradication Actions**: Measures taken to remove the root cause of the breach, such as removing malware or blocking unauthorized IP addresses.
- **Recovery Actions**: Steps taken to restore systems and services to normal operation, including data restoration from backups and system integrity checks.
- **Notifications Sent**: Details of notifications sent to affected individuals, regulators, or other authorities, as required by law.
- **Follow-Up Actions**: Actions taken to prevent similar breaches in the future, such as implementing new security controls or providing additional training.
- **Status**: The current status of the breach, indicating whether it is Open (still under investigation or mitigation) or Closed (resolved).

- **Review Date**: The date the incident will be reviewed to ensure all necessary follow-up actions have been taken.

Usage and Maintenance

1. **Updating the Log**: This log should be updated as new information becomes available and as actions are taken in response to the breach.
2. **Retention**: Data Breach Logs should be maintained for a minimum of [retention period, e.g., five years] in compliance with MOALD guidelines and legal requirements.
3. **Periodic Review**: Conduct periodic reviews of the log to identify patterns and improve incident response processes.
4. **Access Control**: Access to the Data Breach Log should be restricted to authorized personnel to maintain the confidentiality of sensitive information.

APPENDIX U: MOALD- DATA AND INFORMATION SECURITY POLICY STATEMENT

MINISTRY OF AGRICULTURE & LIVESTOCK DEVELOPMENT

1.0 Introduction

This data and information security policy statement outlines MOA&LD's approach to data and information security management. It provides the guiding principles and responsibilities necessary to safeguard the security of MOA&LD's data and information as well as the systems data collection and management.

2.0 Purpose

The Data and Information Security Policy is written pursuant to the Data Protection Act Section 41 and 42 requires the MoALD's data controller or data processors to take measures, in particular: (a) to identify reasonably foreseeable internal and external risks to personal data under the person's possession or control; (b) to establish and maintain appropriate safeguards against the identified risks; (c) to the pseudonym misation and encryption of personal data; (d) to the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (e) to verify that the safeguards are effectively implemented; and (f) to ensure that the safeguards are continually updated in response to new risks or deficiencies. The purpose of the data and information security policy is to provide a framework for establishing suitable levels of information security for all MOALD data and information assets and to mitigate the information security risks associated with the theft, loss, misuse, damage or abuse of these information assets. This policy is an integral part of the KIAMIS data management framework.

3. Scope

This policy governs all data and information that is created, transmitted, processed, stored or disposed during the KIAMIS implementation, information assets and the systems used to create and maintain that information. It applies to:

- All MOALD staff, Counties, partners, suppliers and contractors with respect to information assets;
- Employees, representatives & agents from other organizations who directly or indirectly support MOALD's e.g auditors and other external consultants;
- This policy applies to all MOALD physical and electronic information assets
- The development, implementation, procurement, operation and support and any other activities involving the use of MOALD

4. Policy Statement

MOALD Senior Management Team and KIAMIS Secretariat shall be committed to the implementation and continual improvement of a robust Data and Information Security Management System that ensures appropriate data and information confidentiality, integrity and data availability. The farmers, staff and other sensitive information will be protected against unauthorized access and the integrity of data shall be maintained in line with the KIAMIS Data Governance Framework. Data and information will only be made available to authorized Data processors and controllers through legally binding Non-Discloser Agreements. It is the responsibility of ALL national and county staff members responsible for data collection and management to:

- Ensure that data and information confidentiality is kept and protected against any unauthorized access;
- Ensure integrity of KIAMIS database through protection from unauthorized modification.
- Availability of MOALD data and information to authorized users when needed.
- Protect the Confidentiality, Integrity and Availability of all MOALD data and information assets
- Report any security incident or breach for investigation in accordance with the existing incident management process.

It is the responsibility of ALL directors and top level managers to:

- Implement this policy within their Departments, units or projects and make sure it is adhered to by their members of staff.
- Make sure that all staff within their Departments, Units or Projects undergo appropriate security awareness and/or training in support of the goals of this policy statement.
- Ensure the building of a data and information security culture within MOALD via effective application of data and information security controls and process handling
- Ensure continual improvement of DISMS through process refinement, risk mitigation controls enhancement, effective non-conformity handling and compliance to all associated regulatory requirements.

To support this policy:

- MOALD shall establish and maintain Data and Information Security Management System (DISMS) which incorporates a formal and systematic approach to data and information risk.
- Performance of the DISMS shall be monitored and checked on an annual basis, supported by a set of key performance indicators (KPIs). The performance shall be reported and subject to Management Review
- MOALD shall review the DISMS to identify areas of improvement that ensure the ongoing adequacy and suitability of the DISMS towards meeting its objectives.

DOCUMENT CONTROL

ACTION	NAME	POSITION	SIGN	DATE
Developed by				
Reviewed by				
Approved by				
Effective date				

REVISION HISTORY

REVISIONS				
NO	**DATE OF APPROVAL**	**REVISION NO**	**AMENDED PAGES (ARTICLE)**	**TYPE OF AMENDMENT**
1				

Signed by:

Dr. Andrew Mwihia Karanja, PhD

Cabinet Secretary, Ministry of Agriculture and Livestock Development

APPENDIX V: INCIDENT RESPONSE PLAN (IRP)

MINISTRY OF AGRICULTURE & LIVESTOCK DEVELOPMENT

1. Purpose

The purpose of this Incident Response Plan is to establish a systematic approach for responding to data breaches and security incidents that affect the Ministry of Agriculture and Livestock Development, Kenya. This plan outlines procedures for containing incidents, mitigating risks, and notifying relevant stakeholders to protect sensitive information and maintain public trust.

2. Scope

This plan applies to all departments, systems, and personnel within the Ministry that process or have access to personal and sensitive data. It includes procedures for addressing both electronic and physical data breaches and security incidents involving internal staff, contractors, and third-party service providers.

3. Definitions

- **Data Breach**: Any incident that results in the unauthorized access, disclosure, alteration, or destruction of personal or sensitive data.
- **Security Incident**: An event that could harm the confidentiality, integrity, or availability of the Ministry's information, systems, or services.
- **Incident Response Team (IRT)**: A designated group responsible for managing and coordinating the response to data breaches and security incidents.

4. Incident Response Team (IRT)

The IRT consists of members from key departments within the Ministry, including IT, Legal, Communications, and Human Resources, as well as relevant sector representatives.

4.1 IRT Roles and Responsibilities

- **Incident Response Manager**: Leads the incident response, makes decisions on containment and mitigation, and liaises with executive management.
- **IT Security Officer**: Investigates technical aspects, contains the breach, and supports remediation efforts.
- **Legal Advisor**: Provides guidance on regulatory requirements and compliance, and assists with reporting obligations.
- **Communications Officer**: Manages internal and external communications and ensures that information is accurate and timely.
- **Human Resources Officer**: Addresses any staff-related issues and coordinates internal notifications.
- **Data Protection Officer (DPO)**: Ensures data protection compliance, handles communications with relevant regulatory authorities, and assists in preparing reports.

5. Incident Response Phases

5.1 Preparation

- Ensure all Ministry personnel undergo regular training on data protection, security awareness, and incident reporting protocols.
- Maintain an inventory of key systems and data repositories, and ensure up-to-date contact lists for internal teams and external stakeholders, including law enforcement and regulatory bodies.

5.2 Identification

- Establish a process for detecting and reporting incidents, including monitoring and alerting systems.
- All suspected incidents should be reported immediately to the IRT via the Ministry's official reporting channels (e.g., hotline or dedicated email).
- The IT Security Officer will conduct a preliminary assessment to verify whether a data breach or security incident has occurred.

5.3 Containment

- **Immediate Containment**: Disconnect affected systems from the network to prevent further access or damage.
- **Short-Term Containment**: Apply temporary fixes and restrictions to contain the incident, such as isolating affected servers or workstations.
- **Long-Term Containment**: Implement lasting solutions, including applying patches, updating access controls, and reconfiguring system settings as needed.

5.4 Eradication

- Identify the root cause of the incident, such as malware or unauthorized access points.
- Remove malicious code, unauthorized access methods, or compromised accounts from affected systems.
- Conduct a thorough verification to ensure all threats have been eliminated and systems are secure.

5.5 Recovery

- Restore data and systems from backups as necessary.
- Monitor restored systems for any signs of abnormal behavior to confirm that all issues have been resolved.
- Gradually reintroduce affected systems back into the Ministry's network environment.

5.6 Post-Incident Review

- Conduct a comprehensive review within 14 days of incident resolution, involving all relevant stakeholders.
- Document lessons learned, identify any weaknesses in the response process, and implement improvements to enhance future responses.
- Update the Incident Response Plan and other related policies based on review findings.

6. Reporting Protocols

- **Internal Reporting**: All incidents must be reported to the IRT and relevant department heads immediately upon identification.
- **External Reporting**: If the incident involves personal data, the DPO must assess whether it meets criteria for notifying data protection authorities and other relevant regulatory bodies within 72 hours.
- **Notification to Affected Individuals**: If there is a significant risk to individuals' rights and freedoms, notify affected parties promptly, providing information on how they can protect themselves and contact details for more information.
- **Law Enforcement Notification**: The Legal Advisor, in consultation with the IRT, will determine the need to notify law enforcement authorities if criminal activity is suspected.

7. Communication Plan

- **Internal Communications**: The Communications Officer will work with HR to coordinate messages for employees, providing timely updates and guidance as necessary.
- **External Communications**: All public and media statements will be managed by the Communications Officer, with information verified by the Incident Response Manager to ensure accuracy and compliance.
- **Documentation**: Maintain detailed logs of all activities and decisions taken during the incident, including communication records, which will be retained for a minimum of five years or as required by law.

8. Data Retention and Archiving

- Incident records, including investigation reports, communications, and action logs, will be archived securely for a period of [retention period] and will be made available for future audits and legal reviews.

9. Training and Awareness

- The Ministry will conduct regular training sessions for all personnel on incident detection, reporting, and response procedures.
- The IRT will participate in annual incident response drills and tabletop exercises to ensure readiness.

10. Plan Review and Updates

- This Incident Response Plan will be reviewed annually or following any significant incident. Updates will be communicated across the Ministry to ensure continued alignment with regulatory requirements and best practices.
- The Ministry will engage in regular audits to evaluate the effectiveness of the plan and ensure compliance with national and sector-specific regulations.

APPENDIX W: DATA PROTECTION RISK ASSESSMENT

MINISTRY OF AGRICULTURE & LIVESTOCK DEVELOPMENT

Purpose

The purpose of this Risk Assessment is to identify, evaluate, and mitigate risks associated with the handling of personal data within the Ministry of Agriculture and Livestock Development. This assessment ensures compliance with data protection regulations and enhances the security of sensitive information.

Scope

This Risk Assessment applies to all departments and personnel within the Ministry that handle personal data, covering all systems, processes, and third-party interactions involving data processing activities.

Risk Assessment Process

1. **Risk Identification**: Identify potential risks that could threaten the confidentiality, integrity, and availability of personal data.
2. **Risk Analysis**: Assess the likelihood and impact of identified risks to prioritize them accordingly.
3. **Risk Evaluation**: Determine the acceptable level of risk and identify mitigation strategies for high-priority risks.
4. **Risk Treatment**: Implement mitigation measures and monitor their effectiveness over time.

Risk Assessment Template

Risk ID	Risk Description	Likelihood (Low/Medium/High)	Impact (Low/Medium/High)	Risk Level (Low/Medium/High)	Mitigation Strategies	Responsible Person/ Department	Review Date	Status

Risk Assessment Explanation

- **Risk ID:**A unique identifier for each identified risk.
- **Risk Description:** A detailed description of the potential risk that could impact data protection.
- **Likelihood:** An assessment of the probability of the risk occurring, categorized as Low, Medium, or High.
- **Impact:** An assessment of the potential consequences or damage if the risk were to occur, categorized as Low, Medium, or High.
- **Risk Level:** The overall risk level based on the combination of likelihood and impact, categorized as Low, Medium, or High.
- **Mitigation Strategies:** Specific actions that will be taken to mitigate the identified risk, including preventive measures and response plans.
- **Responsible Person/Department:** The individual or department accountable for managing the risk and implementing mitigation strategies.
- **Review Date:** The scheduled date for reviewing the risk assessment and evaluating the

effectiveness of the mitigation strategies.

- **Status:** The current status of the risk (e.g., Open, Mitigated, Closed).

Risk Management Procedure

1. **Regular Review**: This Risk Assessment will be reviewed at least annually or after any significant incident to ensure it remains current and effective.
2. **Employee Training**: All personnel will receive training on data protection and risk management to enhance awareness and compliance.
3. **Documentation**: Maintain detailed documentation of all risk assessments, reviews, and mitigation activities for audit purposes.
4. **Continuous Improvement**: Monitor the effectiveness of mitigation strategies and update them based on feedback, incidents, or changes in the regulatory environment.

APPENDIX X: DATA PROTECTION & PRIVACY TRAINING RECORDS

MINISTRY OF AGRICULTURE & LIVESTOCK DEVELOPMENT

Introduction

The Ministry of Agriculture and Livestock Development maintains these training records to document and verify that employees, contractors, and relevant third-party personnel have received data protection and privacy training. This log supports compliance with data governance and regulatory requirements.

Training Record Template

For each training session, record the details as follows:

Date of Training	Training Topic	Trainer Name	Participant Name	Job Title	Department	Completion Status	Assessment Score	Certification Issued	Follow-Up Actions

Description of Training Record Fields

- **Session ID**: A unique identifier for each training session.
- **Date of Training**: The date on which the training session was conducted.
- **Training Topic**: The specific subject covered in the training session (e.g., Data Protection and Privacy Awareness, Secure Data Handling).
- **Trainer Name**: The name of the individual or organization that conducted the training session.
- **Participant Name**: The name of the employee, contractor, or third-party personnel who attended the training session.
- **Job Title**: The participant's job title, which helps align training relevance with their responsibilities.
- **Department**: The department or division within the Ministry to which the participant belongs.
- **Completion Status**: Indicates whether the participant completed the training session successfully.
- **Assessment Score**: The score achieved by the participant in the post-training assessment, indicating their level of understanding.
- **Certification Issued**: Specifies whether a certification or acknowledgment of completion was issued to the participant.
- **Follow-Up Actions**: Any additional steps needed for the participant, such as refresher training, additional modules, or remedial action.

Usage and Maintenance

1. **Updating the Log**: Add new entries after each training session, ensuring details are accurate and up-to-date.
2. **Verification**: Verify each participant's completion status and assessment score before finalizing the log entry.
3. **Retention**: Training records should be retained for a minimum of five years or as per regulatory requirements, allowing for audit and compliance verification.

4. **Access Control**: Access to these records is limited to authorized personnel only, such as HR, the Data Protection Officer (DPO), and designated auditors, to maintain confidentiality.

Reporting and Auditing

- **Annual Review**: An annual review of training records will be conducted to ensure all personnel have received the required data protection and privacy training.
- **Compliance Audits**: Training records are subject to internal and external audits to verify compliance with data protection regulations and organizational policies.
- **Retraining**: Based on assessment scores and compliance requirements, personnel may be scheduled for additional or refresher training sessions.

APPENDIX Y:DATA PROTECTION CONSENT FORM

MINISTRY OF AGRICULTURE AND LIVESTOCK DEVELOPMENT

1,0 Overview

The Ministry of Agriculture and Livestock Development uses a **One-off Consent** (OOC) in which the respondents and participants in personal data collection are asked to consent to taking part in the personal data collection only once. This done at the beginning of the respondent's interview before the data is collected.

To get the One-Off Consent, the interviewer is required to read out loud, the data protection consent form and ensure the message is read in the language that the respondent is most familiar with.
The respondent may require copy of the data protection consent form. The enumerator should provide the form is asked for. To facilitate this, enumerators should upload copies of the consent form and share with respondent through WhatsApp, email or other convenient means.

2.0 Ministry of Agriculture and Livestock Development Personal Data Protection Consent Form

Opening Statement **The Ministry of Agriculture and Livestock Development strictly follows the Dat Protection Act 2019 when collecting any kind of personal data. According to the Act, we can only collect your personal data if you understand: our legal and legitimate mandate for collecting the data, why we collect the data, where we keep the data, how we process and use the data, how we share the data with a third party, how you can check, amend or withdraw the information you have given us. According to the Data Protection Act, I can only proceed with the data collection if you consent. I now want to read out to you our personal data protection form. Please listen carefully and feel free to ask any questions or clarifications.**		
Issue	**Explanation**	**Notes for enumerators**
Legal and legitimate mandate:	The MoALD is a constitutional office established and organized to support the government functions in line with the Presidential executive orders.	*Ensure the respondent knows the legal basis why the Ministry and county governments exist*
Purpose of Data Collection:	The purpose of collecting the data is to enable the national and county governments to develop policies and strategies that support farmers' interests and promote agriculture. The farmers support services include but not limited to: provision of targeted subsidies, advisory services on good farming practices; access to market information; support to international trade regulations and traceability requirements; agricultural produce quality standards and postharvest loss mitigation, among others. To support the farmer, the ministry will process the	*Clearly state why the data is being collected and how it will be used.*

	data collected. This involves organizing the data into counties, sub-counties, and wards; categorizing data by value chains, categorization by sizes of farming, flagging out personal and sensitive data, among others.	
Types of Data Collected:	During this exercise, the personal data we will collect from you include: name, ID number, telephone number, land ownership and utilization, the crops, livestock or fish value chains you are engaged, the GPS location of the farm. Other personal data to be collected include.....	*Specify the categories of personal data being collected*
Data Subject Rights:	Under the Data Protection Act 2019, you have a right to know who we are, why we collect your data, where we keep the data, how we share the data with a third party (if needed), how you can correct or amend your data. My supervisors name is: Dr/Mr/Madam/Ms..... Telephone number.....	*Outline the rights individuals have regarding their personal data, such as access, rectification, erasure, and the right to complain to a supervisory authority*
Withdrawal of Consent:	During the interview, feel to stop or ask for clarification about any information you are providing. You are also free to withdraw any information you have given. However, failure to provide the information will severely affect the policies and plans by the government to support Kenyan farmers and address their critical needs.	*Provide information on how individuals can withdraw their consent at any time and the implications of doing so*
Data safety and Retention Period:	The data collected by the Ministry is kept in a central server found at KALRO HQ offices. The Data centre has all the security measures against eraser, antiviruses, antifire, modern cyber security measures, among others. The data collected will be kept for a maximum of ten years. During this period, you are free to access and amend your personal data.	*Explain where the data will be kept, data safety and how long the data will be stored*
Third-Party Sharing:	The data collected may be shared with a third party. These may include another organization, research institute, private company, and so on. Where third party data sharing is done, all the datasets will be anonymized and encrypted to prevent sharing of your sensitive data.	*Clarify whether data will be shared with third parties and under what circumstances.*
Assurance of your personal interests	The government will not use this data to collect taxes, discriminate against you, jeopardize your farming business and competitive edge; share your farming business secretes, negatively affect your farming progress. This consent form is a public document. I can share it with you through your WhatsApp, email or other means if you need it.	*Provide detailed assurance on data use to minimize consent refusal* *If respondent wants copy of the consent form, give him/her through most*

		convenient means.
Contact information	The physical address of the Ministry is..... and the official telephone numbers are..... At the county level, the office is located at..... and the official telephone number is/are..... You are free to check and call the numbers	
Confirmation of Understanding	Do you have any questions regarding the purpose of this exercise and collection of personal data? Do you now allow me to proceed with the interview?	*1 = Yes; 2= No* *If NO, do not proceed with the interview*