K-STATE DATA GOVERNANCE PROGRAM

MISSION AND GUIDING PRINCIPLES

Mission

The mission of the Data Governance Program at K-State is aligned with the university's priorities. The program's primary goal is to enable and promote data-informed decision-making across the campus through focusing on the following key objectives:

1. ***Data Identification:*** The program aims to identify existing data and determine what data will be needed in the future. This process involves understanding the types of data that are crucial for making informed decisions within the university.
2. ***Responsibility:*** It defines the responsibilities related to data management. This step involves specifying who is responsible for collecting, maintaining, and ensuring the quality of data.
3. ***Accountability:*** The program assigns accountability for these responsibilities to specific groups or individuals within the university. This is crucial for ensuring that there is a clear chain of responsibility for data-related tasks.
4. ***Enterprise Perspective:*** The program provides an enterprise-wide perspective on governing data. It takes into account the entire university, rather than just individual departments or units. This holistic approach is important for consistent and effective data governance.
5. ***Institutional Focus:*** It's important to note that the Data Governance Program is primarily a business process that supports the university to achieve its various strategic and business goals. Technology serves as an important enabler and infrastructure to support overall institutional data management.
6. ***Continuous Improvement:*** The Program recognizes that data governance is an ongoing effort. It requires continuous monitoring, modification, and improvement to ensure that data remains accurate, secure, and aligned with the university's goals.

In summary, the Data Governance Program at K-State is designed to create a structured and comprehensive approach to managing data across the university. It is a journey and will require continuous improvement and maintenance to adapt to evolving data needs and challenges.

Guiding Principles

Developing guiding principles helps ensure that data-related activities align with the data governance program's mission and objectives. These principles include:

1. **Data Recognition:** Data is a strategic asset for effective decision-making and cost reduction.
   1.1. *Transparency* - builds trust and encourages collaboration among those involved in data governance.
   1.2. *Consistency* – to ensure fairness and equitable treatment of data where rules are acknowledged and followed. Reduces the possibility of bias and confusion in the workplace.
2. **Clear Accountability:** Data owners and stewards must manage data use and classification.

2.1. *Stewardship* - safeguarding data privacy, security, and confidentiality is a collective responsibility.
2.2. *Accountability* - individuals taking responsibility for their actions, with workplace decisions and processes subject to audits.

3. **Cross-Functional Perspective:** Data should not be isolated, and shared knowledge is vital.
   3.1. *Agility* - ability to adapt and respond quickly to evolving data governance processes and practices. It encourages flexibility and adaptability to meet evolving needs and challenges.
   3.2. *Change Management* - involves effectively communicating, training, and supporting staff to understand, adopt, and integrate new processes into the organizational culture.
4. **Data Integrity:** Ensure consistent data quality throughout its lifecycle.
   4.1. *Consistency* – to ensure all data are in uniform to reduce possible errors during its lifecycle.
   4.2. Accountability - ensures that individuals are held responsible for their duties and errors.
5. **Regulatory Compliance:** Adhere to internal and external rules for data security.
   5.1. *Transparency* - clear communication and openness in decision-making,
   5.2. *Accountability* - all employees take responsibility for their data management decisions and actions emphasizing the consequences of data-related actions for security and regulatory adherence.

K-STATE INSTITUTIONAL DATA POLICY

Rationale/Purpose of the Policy

The value of data as an institutional resource is increased through its widespread and appropriate use; its value is diminished through misuse, misinterpretation, or unnecessary restrictions to its access. As the caretaker of institutional data, the university has an obligation to protect the integrity and quality of institutional data, privacy of data subjects, and security of institutional data while also maximizing its effective and efficient use. The purpose of this policy is to establish minimum requirements for the management and stewardship of institutional data resources.

Definitions

Data domain

A high-level functional category, as designated by the Data Governance Committee, for the purpose of assigning accountability and responsibility for institutional data. Each data domain has a data custodian.

Data lifecycle

Includes data planning, design and enablement, creation and acquisition, storage and maintenance, transmission, use, enhancement, retention and disposition.

Institutional data

Information, regardless of medium, generated, collected, stored, maintained, transmitted, enhanced, or recorded by or for the university to conduct university business. It includes data used for planning, managing, operating, controlling, or auditing university functions, operations, and mission. Examples of Institutional data include student enrollment and demographic information, employee records and demographic information, budget and finance data.

It does not include data generated by research (governed by the office of VPR), or data owned or generated by a party outside the university when used in research, conducted at the university, under the auspices of the university, or with university resources.

Institutional data product

Include, but are not limited to, databases, tables, reports, models, analyses, dashboards, and visualizations that either use or are based on institutional data sources and display or convey representations of institutional data, regardless of format.

Protected institutional data

Institutional data that is not specifically classified as "public" under the university's Data Classification policy PPM 3433.052

System of record (Source)

The single system deemed to be the university's authoritative instance of a particular data element where data is created, captured and/or maintained through a defined set of rules. To ensure data integrity, there must be one system of record for a given data element.

Scope

This policy applies to:

- All institutional data and institutional data products regardless of where they reside.
- All information systems and applications that generate, collect, store, maintain, transmit, or record institutional data; regardless of system and application manager, steward, or location, or support information systems and applications that generate, collect, store, maintain, transmit, or record institutional data.
- All individuals, regardless of affiliation, who handle, use, process, store, or manage institutional data.

Policy Statement

I. **Institutional data shall be treated as a shared university resource** and as with all types of data across the various divisions, colleges, and campuses at K-State, it is a valuable resource that belongs to the institution. University data custodians and stewards are responsible for managing all data for the benefit of the whole university including

supporting the university's mission and facilitating campus-wide data-informed decision-making activities.

Guiding principles for the management of institutional data are:

A. Stewardship: All individuals within the scope of this policy have a responsibility to protect the privacy, security, and confidentiality of our institutional data as required, and to manage it appropriately throughout the whole data lifecycle.

B. Consistency: Procedures and standards shall be thoughtfully created and applied uniformly to provide consistency in how institutional data is managed across the university.

C. Accountability: Progress toward institutional data management goals shall be measured and tracked and compliance with policies, procedures, and standards shall be auditable in accordance with current data governance best practices.

II. **Institutional data shall be responsibly managed throughout the entire data lifecycle** in compliance with all applicable federal and state laws; Kansas Board of Regents, and university policies, procedures, and standards; and approved records schedules. Institutional data stewards serve as the primary point of contact and coordination for data management issues and operations within the steward's data domain.

III. **Institutional data shall be identified and documented.** Institutional data sources, elements, processes, integrations, and products will be documented and communicated to ensure clarity, shared understanding, and availability.

IV. **Access to protected institutional data shall be authorized and managed** to protect individual privacy, maintain promised confidentiality, and ensure appropriate access and use. Access will be granted based on authorization provided by the applicable institutional data steward or stewards based on appropriateness of an individual's role and the intended use. Authorization and access will be documented, reviewed, modified, and terminated in accordance with all applicable laws and university policies, procedures, and standards.

V. **Access** to and the use of individual and/or sensitive information based on a user's justifiable business needs should be approved by system steward. The quality and integrity of institutional data and institutional data products shall be actively managed and explicit criteria for data validity, availability, accessibility, interpretation, and ease of use shall be established.

VI. **Units** across the universities should make bona fide efforts to eliminate unnecessary redundant systems that may result in greater confusion, undermining data consistency, and an ineffective use of university resources.

VII. **Institutional data shall be classified in accordance with applicable university data classification policy.** Determination of appropriate classification of institutional data and institutional data products shall be made and documented by data stewards. Data

classification will be a factor considered in authorization and access procedures. {PPM 3433}

A. Data classifications may hold multiple definitions and fall into a variety of categories and laws, such as items like directory information, which encompass various levels of Personal Identifiable Information (PII) data that may have different uses, definitions, and interpretations under the rules of law (e.g., FERPA – student directory information, KS Statute 21-6107).

VIII. **Any system holding institutional data shall be purposefully planned, inventoried, and implemented** to manage institutional data throughout the entire data lifecycle in compliance with all applicable federal and state laws; Kansas Board of Regents, and K-State policies, procedures, and standards; and approved records schedules.

IX. **Institutional data products shall source institutional data from systems of record.** Institutional data resources and products that are published, distributed, shared, or otherwise made accessible to others will source institutional data from designated systems of record, including university data warehouse.

X. **Data preservation** is the act of conserving and maintaining both the safety and integrity of data. Preservation is done through formal activities that are governed by policies, regulations and strategies directed towards protecting and prolonging the existence and authenticity of data and its metadata (also see PPM 3090).

XI. **Data governance groups, unit leaders, and policy managers** should carefully monitor the ethical aspects and new development in the AI world.

XII. **Exceptions to this policy may be granted by the policy manager.** In certain situations, compliance with this policy may be impossible, may not be immediately possible, or may constitute an undue administrative or financial burden. In such cases, exceptions to this policy may be granted by the policy manager in consultation with the appropriate data steward(s) and Data Governance Committee. Exceptions must be documented and be time bound when appropriate. A denial of a request for an exception may be appealed to the Data Governance Committee.

XIII. **Violations of this policy may result in a range of consequences.** Compliance with this policy is designed, in part, to ensure the university complies with its various data-related obligations, including legal and regulatory requirements.

XIV. **Procedures, standards, and guidelines will be developed and approved by the Data Governance Committee** to aid in the implementation and enablement of this policy and its principles.

Roles and Responsibilities

Data Governance Steering Committee: The Data Governance Committee consists of designated officials who have planning, policy-level, and management responsibility for data within their functional areas. The Data Governance Committee works to ensure and support the effective

management of data assets of the university by making policy recommendations, establishing procedures and standards, advocating for appropriate resources, and guiding and monitoring data governance efforts.

Data Governance Steward Committee: It would be comprised of Institutional Data Stewards and Data System Stewards from domain areas. To accomplish tasks, the committee may create temporary smaller working groups / task forces composed of Data Steward Team members as needed.

Data Custodians are accountable for the oversight and general operation of institutional data systems that serve a broad section of the university community. It is the responsibility of the Data Custodians to provide direct authority and control over the management and use of institutional data in his/her area of responsibility regardless of which system in which the data resides.

Each custodian appoints one or more institutional data stewards for the data custodian's specific domain.

Institutional Data Steward: This refers to the data stewards who are functioning at an enterprise level and are responsible for defining data policies, procedures, and standards for their assigned data domains across the entire institution. E.g. ERP system -- KSIS, FIS, HRIS

- Key aspects of the Institutional Data Stewards:
  - Assigned by and accountable to the Data Custodians.
  - Responsible for the full lifecycle of data within their domains.
  - Define and enforce data management policies and procedures consistently across their domain.
  - Across the domains and work with IT to implement security controls, access rules for protected data.
  - Closely involved in high-level governance activities like policy development.

Data System Steward: This refers to data stewards who are operating at the ancillary system or application level, responsible for the direct system administration and management of a specific data solution.

E.g. CRM system -- Maxient, Canvas, Slate, Salesforce, Concur, Kronos, etc.

- Key aspects of Data System Stewards:
  - Manage day-to-day system operations, maintenance, uptime.
  - Support activities like user access provisioning, backup, and recovery.
  - Monitor system resource usage, configuration changes.
  - Implement operational processes, scripts, jobs related to one system.
  - Tactical role focused on keeping the system functional.

Data Governance Manager: Data Governance Manager is responsible for the data governance framework.

Data Producer: Data Producer is responsible for creating and capturing data as per standards set by data stewards.

Related K-State Committees

Records and Information Management Committee

Faculty Senate Committee on Technology

IT Security Committee Data/Cyber Security Compliance Group

K-SAC

Related K-State Policies

Retention of Records

Access Authorization to University Digital Data and System

Financial Information System Policy

Data Classification and Security

University Handbook, F41: Student Records

Use of University Mobile Devices, Personal Devices, and Accounts Policy

---

Policy Administration and Review

Approval Authority: Provost and Executive Vice President

Policy Manager: Chief Data Officer

Policy Coordinator and Contact: Director, Data Governance and Policy

Policy Review: This policy is reviewed at least annually

Acknowledgement: This policy has been developed by duplicating with permission certain sections of University of Wisconsin-Madison's data policy.