ITEC Policy 8010 - Kansas Data Review Board Policy

1.0 TITLE: Kansas Data Compliance Requirements

1.1 EFFECTIVE DATE: July 1, 2021

Revised: March 9, 2021

1.2 TYPE OF ACTION: New Policy

2.0 PURPOSE: To define the policy and requirements for Kansas data management for all agency business and information technology initiatives and acquisitions. This policy will also define required controls to establish formal oversight of the people, processes, and technologies that influence data throughout its lifecycle, with the intent of reducing risk and improving outcomes of processes that depend on or use data. These requirements will provide increased assurance that data is reliable, accurate, timely, fit for use, interoperable, consistent, and protected from loss and unintended disclosure or alteration.

3.0 ORGANIZATIONS AFFECTED: All branches, boards, commissions, departments, divisions, and agencies of state government, hereafter referred to as Entities.

3.1 This policy applies to all employees and contractors within State Budget Units (BUs) who work with data or repositories of data while executing business functions, activities or services for or on behalf of the BU or its customers.

3.2 Applicability of this policy to third parties is governed by contractual agreements entered into between BUs and the third party. For contracts in force as of the effective date, subject matter experts (SMEs) acting under the guidance of the Kansas Data Review Board (KDRB) should ascertain the applicability of this policy to third parties before seeking amendments. Prior to entering into new contracts, SMEs shall ascertain the applicability of this policy to third parties and include compliance requirements in the terms and conditions.

3.3 Applicability of this policy to specific information systems shall be determined by the Kansas Data Review Board (KDRB) as defined below. BUs may implement additional controls, roles, or organizational structures as they deem necessary to suit their business or project needs.

4.0 REFERENCES:

4.1 K.S.A. 75-7203 authorizes the ITEC to: Adopt information resource policies and procedures and provide direction and coordination for the application of the state's information technology resources for all state entities.

5.0 DEFINITIONS:

5.1 Data governance encompasses the people, processes, and technologies required to create, manage, and protect an organization’s information throughout its lifecycle. By implementing a data governance program, an agency ensures consistent, secure data is available to multiple departments as well as other state agencies. This allows agencies to more effectively fulfill their missions while ensuring the safety and privacy of their agency, employees, and constituents. Additional benefits include:

* Improved operational efficiency
* Improved standardization and understanding of data
* Reduced data management and storage costs
* Better decision-making
* Better regulatory compliance

5.2 Data compliance is the practice of ensuring that sensitive data is organized and managed in such a way as to enable organizations to meet enterprise business rules along with legal and governmental rules. In general, compliance means conforming to a rule, such as a specification, [standards](https://en.wikipedia.org/wiki/Policy), standard, or law.

Regulatorycompliance describes the goal that organizations aspire to achieve in their efforts to ensure that they are aware of and take steps to comply with relevant [laws](https://en.wikipedia.org/wiki/Law), policies, and [regulations](https://en.wikipedia.org/wiki/Regulations). Due to the increasing number of regulations and the need for operational transparency, organizations are increasingly adopting the use of consolidated and harmonized sets of compliance controls. This approach is used to ensure that all necessary governance requirements can be met without the unnecessary duplication of effort and resources.

Regulations and accrediting organizations vary among fields, with examples such as the Payment Card Industry Data Security Standard (PCIDSS) and the Gramm-Leach-Bliley Act (GLBA) in the financial industry, the Federal Information Security Management Act (FISMA) for U.S. federal agencies, the Hazard Analysis Critical Control Point (HACCP) for the food and beverage industry, and the Health Insurance Portability and Accountability Act (HIPAA) in healthcare. In some cases, other compliance frameworks (such as Control Objectives for Information and Related Technology or COBIT) or policy (such as the National Institute of Policy and Technology or NIST) detail how to comply with regulations.

Some organizations keep compliance data—defined as all data belonging or pertaining to the enterprise or included in the law, which can be used for the purpose of implementing or validating compliance—in a separate data warehouse for meeting reporting requirements. Compliance software is increasingly being implemented to help companies manage their compliance data more efficiently. Compliance data may include calculations, data transfers, and audit trails.

5.3 DATA PRIVACY consists of privacy policy as well as statements or legal documents (in privacy law) that discloses some or all of the ways a party gathers, uses, discloses, and manages a customer or client's data. Personal information can be anything that can be used to identify an individual, not limited to the person's name, address, date of birth, marital status, contact information, ID issue, and expiry date, financial records, credit information, medical history, where one travels, and intentions to acquire goods and services. In the case of a business, it is often a statement that declares a party's policy on how it collects, stores, and releases personal information it collects. It informs the client what specific information is collected, and whether it is kept confidential, shared with partners, or sold to other firms or enterprises. Privacy policies typically represent a broader, more generalized treatment, as opposed to data use statements, which tend to be more detailed and specific.

These are the most basic elements that a privacy policy should include:

* Who is the site/app owner?
* What data is being collected? How is that data being collected?
* What is the Legal basis for the collection? (e.g consent, necessary for your service, legal obligation etc.) -This is...
* For which specific purposes are the data collected? Analytics? Email Marketing?

5.4 RECORDS MANAGEMENT refers to the systematic and administrative control of records, including data, throughout their life cycle. Data should be appraised according to its administrative, fiscal, legal, and historical value and scheduled accordingly. All data created or received by an agency must be covered by a retention schedule describing the data and listing a retention period, disposition, and any access restrictions. Data which has not been scheduled shall not be destroyed.

6.0 POLICY, It is the responsibility of each state agency to manage and safeguard its information. In order to safeguard information, these steps should be followed:

1. Collect only data that is necessary for the agency’s mission.
2. Designate a data owner, custodian, and other roles as appropriate.
3. At a minimum Agency Policy and Controls should be reviewed each year by the Data Owner, Data Custodian, Information Security Officer and the Agency Leadership. The reviews should be documented and maintained within the policy and controls itself.
4. Disclose and provide access as appropriate applying the need to know standard.
5. Insure a formal documented agreement is in place for any data that is shared between agencies. Agreements are to have a formal documented reviewed annually.
6. Safeguard data in both transit and at rest applying the appropriate levels of encryption and storage safeguards.
7. Secure physical equipment and resources used for processing and storing data.
8. Retain and dispose of all data securely and in accordance with State Records Board-approved agency retention and disposition schedules.
9. Adhere and comply with all applicable privacy laws.
10. Stay informed about information risks as it relates to any data the agency manages.

6.1 ITEC 7230A 6.3 and 6.4 states entities must ensure that Information Asset Trustees are appointed for Intellectual property or data compilations that contain or may be projected to contain Source Records on thirty (30) or more individuals of Restricted-Use Information.

Depending on the volume and sensitivity levels of the data being managed, some agencies may require more roles than others. At a minimum, agencies must have those roles marked with an asterisk with named and approved individuals.

|  |  |
| --- | --- |
| **Role (Asset Trustees)** | **Responsibility** |
| \*Agency Head | Overall accountability for oversight of state agency data management. |
| \*Information Security Officer | Overall security of agency data and liaison to the Chief Information Security Officer (CISO) of the State of Kansas. Promotes security awareness. |
| Privacy Officer | Provides guidance on privacy laws. |
| \*Data Owner | Security of the data. Accountable to the Agency Head. |
| \*Data Custodian | Protects data from unauthorized access, alteration, destruction, or usage and in a manner consistent with agency policies and policy applicable to the assigned classification level. There are likely to be more than one custodian to represent an agency’s full complement of data assets. |
| \*Records Officer | Ensures an agency’s records are scheduled, retained, and managed in accordance with all state and federal records laws. |
| Data User & End User | Reads and complies with agency data security requirements. |
| System Owner | Develops any additional local requirements, guidelines, and procedures needed to protect the data. |
| Account Administrator | Manages user access and permissions to the data. |

*Data Governance Roles and Responsibilities Matrix*

7.0 PROCEDURES:

7.1 Agencies shall provide a list of individuals assigned to data governance roles to the Chief Information Technology Architect (CITA) each year using the Data Governance Roles and Responsibilities Matrix above by the end of the first month each year.

7.2 Agencies will ensure that personnel assigned to these roles receive role-based training within 30 days of their assignment.

7.3 Agencies storing and collecting data will be able to show an inventory listing of this data that at minimum demonstrates the following:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Data Type** | **Classification** | **Compliance** | **Location** | **Backup Location** | **Shared With** | **Recovery Objective** | **Risk if Breached** |
| Credit Card Information | Restricted | PCI | TODC | TAPE/ Caves | KDOR | 8 hours | HIGH |
| Federal Tax Information (FTI) | Restricted | Pub 1075 | Unisys | Unisys | DCF | 8 hours | HIGH |
| Social Security Information | Restricted | SSA | ESOB | Unisys | DCF | 8 hours | HIGH |
| Personally Identifiable Information (PII) | Restricted | Privacy Laws | ESOB | Unisys | KDOL | 8 hours | HIGH |

8.0 RESPONSIBILITIES:

8.1 The agency Data Owner shall be responsible for the overall agency data program and policies.

8.2 The agency Data Owner or their designee shall be responsible for ensuring the procedures for this policy are completed on time each year.

8.3 The CITA will serve as the state’s principal Data Steward towards the goals of promoting best practice management of the State’s data assets. This includes governance, sharing, privacy, security, compliance, encryption, retention, and disposal.

8.4 The CITA will champion data governance and compliance for the State along with other state officers.

9.0 GUIDES AND AIDS FOR AGENCIES:

9.1 The additional dictionary of terms may be useful in defining a data program:

|  |  |
| --- | --- |
| Access Management | The process of identifying, tracking, controlling and managing authorized or specified users’ access to data in a system. |
| Audit Trail | An electronic or paper log used to track computer activity. This information may include who had access to the data, when, and their reason for requesting access. |
| Collection | The compilation or assembly of data that relates to a particular subject or area. |
| Content Management | The process for collection, delivery, retrieval, governance and overall management of information in any format. |
| Data Administration | An ongoing, centralized, administrative function that coordinates the design, implementation, and maintenance of an effective data structure of the entities and relationships that comprise the integrated enterprise-wide database(s), and makes this information available to a community of information resource users . |
| Data Analytics | The science of examining raw data with the purpose of drawing conclusions about that information. |
| Data Architecture | A set of rules, policies, policy and models that govern and define the type of data collected and how it is used, stored, managed, and integrated within an organization and its database systems. |
| Database | A structured set of data held in a computer, especially one that is accessible in various ways . |
| Data Breach | An incident that involves the unauthorized or illegal viewing, access, or retrieval of data by an individual, application, or service. |
| Data Classification | The process of sorting and categorizing data into various types, forms, or any other distinct class. This process is often used to sort data for security reasons by classifying data into restricted, public, or private data types. |
| Data Integration | The process of retrieving data from multiple source systems and combining it in such a way that it can yield consistent, comprehensive, current, and correct information for business reporting and analysis. The source systems may be various types of devices and the data may be in a variety of formats. |
| Data Integrity | Maintaining data accuracy and consistency over time. |
| Data Modeling | A representation of the data structures in a table for an organization’s database and a powerful expression of the organization’s business requirements. The data model is the guide used by functional and technical analysts in the design and implementation of a database. |
| Data Ownership | The process of assigning formal accountability over a single piece of data or set of data elements with the purpose of ensuring complete control over the data. Data ownership defines and provides information about the rightful owner of data assets, which is the individual or team that implements data acquisition, use, and distribution policies for the data for which they are accountable. |
| Data Privacy | The aspect of information technology that deals with the ability of an organization or individual  to determine what data in a computer system can be shared with third parties. |
| Data Quality | An intricate way of measuring data properties from different perspectives.  It is a comprehensive examination of the application efficiency, reliability, and fitness of data, especially data residing in a data warehouse. |
| Data Repository | A place that holds data, makes data available to use, and organizesdata in a logical manner. Adata repository may also be defined as an appropriate, subject-specific location where researchers can submit their data . |
| Data Security | Protective digital privacy measures that are applied to prevent unauthorized access to computers, databases, and websites, and to protect associated data from corruption. |
| Data Standard | Documented agreement on the format and definition of common data. Established consistent specifications for data elements, such as the name of the data standard, definition, field length, and other components. |
| Data Stewardship | The formalization of accountability over the management of data and data-related assets. |
| Data Visualization | The process of displaying data and/or information in graphical charts, figures and bars. It is used as a means to deliver visual reporting to users for the performance, operations, or general statistics of an application, network, hardware, or virtually any IT asset. |
| Data Warehouse | A technology that aggregates structured data from one or more sources so that it can be compared and analyzed for greater business intelligence. |
| Document vs. Data | A document merges data and format together to assist the reader in understanding the context of the data. A document is usually a set of words that form sentences that can be understood in their form and context. Data usually does not contain syntax or grammar, leaving the letters and numbers without association beyond the database schema or data dictionary. |
| Historical Data | Collected data about past events and circumstances pertaining to a particular subject. |
| Master Data | The core data that is essential to operations in a specific business or business unit. Master data are data units that are non-transactional, top level, and relational business entities or elements that are joinable in observable ways. |
| Metadata | Structured information that describes, explains, locates, or otherwise makes it easier to retrieve, use, or manage an information resource. It is data that provides information about data. |
| Personally Identifiable Information  (PII) | Information that, when used alone or with other relevant data, can identify an individual. PII may contain direct identifiers that can identify a person uniquely or quasi-identifiers that can be combined with other quasi-identifiers to successfully recognize an individual. |
| Sensitive Data | Data that is private, personal, or proprietary and must be protected from unauthorized access. |
| Structured Data | Data that has been organized into a formatted repository, typically a database, so that its elements can be made addressable for more effective processing and analysis. |
| Transactional Data | The information recorded from transactions. A transaction is a sequence of information exchange and related work (such as database updating) that is treated as a unit for the purposes of satisfying a request. |
| Unstructured Data | Information, in many different forms, that doesn’t hew to conventional data models and thus typically isn’t a good fit for a mainstream relational database. |
| Workflow | The movement of data, documents, or tasks through a work process; generally used in the context of technologies that automate workflows. |