Policies

Data Use

Chapter 3420

Created February 14, 2025

Table of Contents

This Data Use Policy (Policy) is intended to safeguard the University from misappropriate use, theft, and/or loss of University Data and Personally Identifiable Information.

For information regarding policy for Information Technology Resources and communications networks, please refer to the Acceptable Use Policy (/policies/ppm/3400/3410.html).

.010 Purpose

The purpose of this Policy is to define the acceptable ways in which data can be accessed, utilized, and shared inside and outside of the University. This Policy will outline the appropriate means by which data and files can safely be managed by university stakeholders and outside entities.

.020 Scope

This Policy applies to all individuals affiliated with the University, including faculty, staff, student workers, contractors, and other affiliates, who access or utilize University data, records, or documents in paper or electronic formats. It encompasses all data created, collected, stored, processed, or transmitted using institutional resources, regardless of format. This Policy also extends to all Information Assets and Information Technology Resources within the University. All members of the University community with access to university data are subject to this Policy.

.030 Definitions

For clarity and to ensure a common understanding of terms used in this policy, please refer to the Glossary of Defined Terms (/it/about/policies/defined-terms-glossary/) which provides detailed definitions for all key concepts and terminology.

.040 Policy

A. **Authorized Data Access:** Access to University data and technology resources is granted to users based on explicit needs for access related to legitimate purposes for administration, education, and research. The University utilizes a data classification system to classify data based on sensitivity and potential impact, and these categories determine the level of protection and access control required.
Access to non-Public data requires authorization by the Institutional Data Steward (or designee) for the related system and/or data. System and/or data access is requested through the System Authorization Process.

The Data Access Manager for the University colleges, divisions, offices, departments, and other units must request access and authorization to data for users under their supervision. Once access is approved, the Data Access Manager will be notified by the Division of Information Technology. The Data Access Managers are also responsible for ensuring termination of access upon departure from their unit (whether transfer, retirement, or other separation).

Data Access Managers are responsible for confirming appropriate and necessary user access. Access should only be granted to users who intend to use the data for university services and business operations.

1. **Data Steward Responsibilities**
Institutional Data Stewards are designated University officials who are responsible for overseeing all data compliance operations within one or more data domains (Financial, Administrative, HR/Personnel, Research). Data Stewards work with the Information Privacy & Security Oversight Committee (IPSOC) or similar body to ensure that appropriate resources are made available to support the data governance needs of the University. Data Steward responsibilities include:

    - Responsible for full lifecycle of data in their assigned domains.
    - Promoting appropriate data use, data integrity, quality, accuracy, and availability through development of standards and procedures.
    - Determining legal and regulatory requirements for data within their area.
    - Supporting the Data Governance Committee in the establishment and implementation of data policies.

    All requests for data access will be routed to the appropriate Institutional Data Steward for review and approval through processes defined in the System Authorization Process.

2. **Data Custodian Responsibilities:** Data Custodians are responsible for the management and operation of data, University systems, networks, and servers that collect, store, transfer, and maintain University Data. Data Custodian responsibilities include:

- Managing data user access in partnership with Institutional Date Steward(s).
- Ensuring data integrity, quality, accuracy, and availability in partnership with Institutional Data Steward(s).
- Work with the Information Security Office to implement security measures to protect data from unauthorized access, disclosure, alteration, or destruction.
- Ensuring data handling practices comply with relevant regulations, laws, policies and standards.
- Managing data user access in partnership with Institutional Date Steward(s).
- Ensuring data integrity, quality, accuracy, and availability in partnership with Institutional Data Steward(s).
- Work with the Information Security Office to implement security measures to protect data from unauthorized access, disclosure, alteration, or destruction.
- Ensuring data handling practices comply with relevant regulations, laws, policies and standards.

3. Data users should seek authorization from the appropriate Institutional Data Steward when requesting access to data outside normal service and business operations scope of work.
4. Data users should seek authorization from the appropriate Institutional Data Steward when unsure of protocols or compliance with sharing data.
5. Institutional Data Stewards must obtain approval from the Data Governance Committee before releasing University data to parties outside of the University.

B. **Data Usage:**
Internal data users must access data only for approved purposes related to their roles and responsibilities within the University. Individual users will be held responsible for using University data and PII appropriately.

- Access to University data and PII by those other than then general users or stewards must:
  - Be for the purposes of furthering the mission of the University.
    - Be for the purposes for which they are assigned.
    - Be in accordance with all license and contractual agreements to which the University is a party.
    - Comply with policies of any network over which such data or information must be routed to reach its final destination.
    - Not interfere with the operation of University Information Technology Resources nor unreasonably interfere with the appropriate use of University Information Technology Resources by other users.
    - Not compromise the security and confidentiality of data that is the property of the University or any other user of University Information Technology Resources.
    - Not attempt to circumvent or subvert any system's security measures.
    - Not represent yourself electronically as another user.
    - Not disrupt services, damage files, or intentionally damage or destroy equipment, software, or data belonging to the University or other users.
    - Not be for personal purpose other than incidental and minimal use.

- Not be for private commercial use unless authorized by contract.
- Not intentionally misrepresent personal identity.
- Be in accordance with applicable state and federal laws (includes such laws as FERPA, Gramm Leach Bliley Act, Digital Millennium Copyright Act, US copyright laws, and policies regarding the protection of data).
- Not conflict with or violate any other University or Kansas Board of Regents policy.

C. **Data Sharing and Transfer:**

- **Electronic**: Any transfer of institutional data must take place via an encrypted channel, both internal and external to the University. Encrypted University data may be transferred via encrypted or unencrypted channels. All email communications to addresses outside of the University environment and contain sensitive data must be encrypted. Please refer to the Data Classification and Storage policy (/policies/ppm/3400/3433.html) for additional details.
- **Physical:** To relocate or transfer data in a physical format, users must place the data on an encrypted external hard drive. If an encrypted storage device is not available or feasible, the data to be transferred must be encrypted before being transferred to the portable storage medium.

D. **Compliance:**
Users are expected to comply with all applicable federal, state, and local law, regulations, and rules, and all University policies regarding university data use. Users are responsible for reporting any suspected misuse. Violations may result in disciplinary action and loss of system access.

Regular compliance checks and audits will be conducted to assess adherence to data access and use policies, with corrective actions taken as necessary. Institutional Data Stewards will request Data Custodians to perform periodic and regular user access reviews for accounts with access to sensitive and restricted data.

E. **Data Use Training and Awareness:**

- **Training Programs**: Regular training sessions on data access, use, and security will be provided to all relevant stakeholders to ensure understanding and compliance.
- **Information Privacy and Security Oversite Committee**: The IPSOC will provide oversight and guidance on data access and use practices, ensuring alignment with regulatory requirements best practices.

.050 Roles and Responsibilities

The Chief Information Officer (CIO) is responsible for the implementation, oversight, and maintenance of this policy. The Vice President for Administration and Finance is responsible for the final approval of this policy.

Any questions about the contents of this policy or the applicability of this policy to a particular situation should be referred to the Office of the Chief Information Officer (CIO).

.060 Exceptions

Exceptions from this policy must be approved as described in the Security Exceptions Management Policy. Any questions about the contents of this policy or the applicability of this policy to a particular situation should be referred to the Office of the Associate Vice President for Information Technology and Chief Information Officer (CIO).

.070 Policy Violations

Failure to comply with university policies may result in the loss of computing privileges, restriction of the ability of devices to connect to or be used on university networks, and other disciplinary measures as defined in Disciplinary Policies and Procedures. Violations may lead to disciplinary actions, including discharge, dismissal, expulsion, legal actions, and criminal investigation or prosecution.

.080 Periodic Review and Policy Updates

To ensure relevance and compliance with evolving regulatory, technological, and operational standards, this policy must undergo a comprehensive review at least annually in accordance with the requirements described in the Policy on Policies. During this review, necessary updates will be made to reflect any new legal requirements, organizational changes, or external factors impacting policy efficacy.

.090 Related Laws and Regulations

- State of Kansas, ITEC Information Technology Policy 7230 Enterprise Security Policy
- State of Kansas, ITEC Information Technology Standards & Guidelines 7230A IT Security Standards

