KENTUCKY STATE UNIVERSITY

Policies and Regulations

POLICY TITLE:
Data Classification

APPLIES TO:
All representatives, affiliates, vendors, and contractors who use, generate, or have access to Kentucky State University data

ADMINISTRATIVE AUTHORITY:
Chief Information Officer (CIO)
Department of Information Technology (IT)

APPROVED BY:
Kentucky State University Board of Regents

EFFECTIVE DATE:
August 8, 2025

NEXT REVIEW DATE:
August 8, 2028

POLICY STATEMENT:

All Kentucky State University (KSU) data must be classified according to its level of sensitivity to ensure that appropriate security controls are applied. This policy provides the framework for classifying data and outlines the baseline requirements for its protection. All users are required to familiarize themselves with and adhere to this policy to protect the university's information from unauthorized disclosure, use, modification, or deletion, and to ensure compliance with applicable laws and regulations.

DEFINITIONS:

Data Classification Level

- **Confidential:** The most sensitive data, intended for use strictly within KSU and protected by law or confidentiality agreements (e.g., data covered by FERPA, HIPAA, GLBA, PCI-DSS). Its unauthorized disclosure

could seriously and adversely impact KSU.

- **Restricted:** Less-sensitive business data intended for internal KSU use. Its unauthorized disclosure could adversely impact KSU or its partners but would not violate the law. By default, all information not defined as Confidential or Public is considered Restricted.

- **Public:** Information approved by KSU administration for release to the general public, which may be disclosed to anyone.

Data Owner
The KSU manager or official responsible for the business function supported by an information resource. Data owners are responsible for authorizing user access and ensuring users are trained on proper data handling.

Data Custodian
An employee responsible for the day-to-day maintenance of information resources, such as backups and physical security. This is a shared responsibility between Information Technology and data owners.

Data User
An individual authorized by a data owner to access university data to perform their job responsibilities.

Information Resources
All data, equipment, facilities, and software used by KSU to create, collect, process, store, and transmit information.

PROCESS:

Guiding Principles
The requirements set forth in this policy are based on the principles of "need to know" and "least privilege." This means information should not be disclosed to any person who does not have a legitimate and demonstrable business need for it.

Data Handling Requirements
All data users must utilize appropriate controls when storing, handling, and distributing KSU information.

Access Control

- Access to information must be granted only to individuals with a legitimate business need and specific authorization from the Data Owner.

- Systems must have controls to authenticate the identity of users before granting access.

- When an employee changes departments or leaves the University, the IT Help Desk must be notified immediately so access can be modified or removed.

Data Transmission

- **Confidential Data:** Must be encrypted when transmitted over any external or wireless network. All such transmissions must use a virtual private network (VPN) or similar IT-approved software. Transmission over personal or non-KSU networks is prohibited.

- **Restricted Data:** Encryption is strongly recommended when transmitting over external or wireless networks.

Data Storage

- All KSU information should be stored on KSU servers, network storage devices, or KSU-approved cloud storage. Storing data on local PC drives is not recommended as it is not backed up.

- Storage of Confidential data on personal or unauthorized equipment is prohibited unless approved by IT, in which case encryption is required.

- Storage of credit card information on KSU computing equipment is prohibited.

Data Disposal

- Storage media containing sensitive (confidential or restricted) information must be completely sanitized or physically destroyed before being reused or disposed of. Deleting files is not sufficient. Users must contact IT for assistance with proper data disposal.

Incident Reporting and Information Requests

- **Loss or Breach:** The loss, breach, or unauthorized access of any Restricted or Confidential data must be reported immediately to Information Technology, the Office of the General Counsel, Risk Management, and the KSU Police Department.

- **Open Records Requests:** All requests for data or information made under the Kentucky Open Records Act must be referred to the Office of the General Counsel.

REFERENCES AND RELATED MATERIALS:

CONTACTS:

Subject	Office	Telephone	E-mail
General Questions	Office of the CIO	(502) 597-7000	Wendy.Dixie@kysu.edu

HISTORY:

Revision Type	Date of Issuance/Revision	Drafter(s)/Editor(s)
Issued (New Policy)	May 2014	Unknown
Revised (New Template and Minor Revisions)	June 2025	Wendy Dixie and Zach Atwell