KENTUCKY STATE
UNIVERSITY
Policies and Regulations

REGULATION TITLE:
Data Security Controls

APPLIES TO:
All users of KSU information technology resources

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

APPROVED BY:
Kentucky State University Board of Regents

EFFECTIVE DATE:
August 8, 2025

NEXT REVIEW DATE:
August 8, 2028

REGULATION STATEMENT:

This regulation implements the Data Security and Management Policy by establishing the specific, mandatory technical controls required to protect university data and information systems.

DEFINITIONS:

Personally Identifiable Information (PII)
Sensitive information that can be used to identify an individual, such as Social Security number, date of birth, and driver's license number.

PROCESS:

Password Security

- Passwords must be treated as confidential information and must not be shared.

- Network passwords are required to be changed every 180 days.

- All password resets are performed by the Information Technology (IT) Help Desk or online. Users must provide proof of identity (e.g., KSU ID number) before a password will be reset.

Workstation and Device Security

- Password-protected screen savers are mandated on all university-owned computers and must be set to a maximum timeout of 15 minutes.

- All KSU information must be stored on university servers, network storage devices, or university-approved cloud storage. Storing KSU information on local PC drives (C: drive), USB drives, CDs/DVDs, or other portable devices is prohibited.

Encryption

- All files containing Personally Identifiable Information (PII) must be encrypted. Instructions for encrypting Microsoft Office documents are to use the "Protect Document" feature under the "File" menu.

- Applications that do not have encryption capabilities must not be used to handle PII.

- PII is not permitted in the body of an email.

- Encrypted files containing PII may be sent via email, but the email must not contain the encryption key or password. The key may be communicated over the phone or in a separate email.

- All backups of PII must be encrypted.

REFERENCES AND RELATED MATERIALS:

- Data Security and Management Policy

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)	June 2025	Zach Atwell