



---

**POLICY TITLE:**

**Information Technology Security**

**APPLIES TO:**

**All users of KSU information technology resources**

**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:**

This policy communicates the security measures required to ensure the appropriate protection and safeguarding of Kentucky State University's (KSU) Information Technology (IT) resources and systems from unauthorized access and misuse. KSU is committed to implementing security measures that ensure the confidentiality, integrity, and availability of its IT resources. Every user of KSU's IT resources bears responsibility for protecting these resources in compliance with this policy and all applicable laws.

**DEFINITIONS:****Information Security Incident**

An actual or suspected event that adversely affects the security of KSU's information resources or systems. Examples include, but are not limited to: website defacement, theft or loss of a computing device containing PII, unauthorized access to data, a computer infected with malware, or a data breach.

### **Information Technology (IT) Resource**

Any data, information, or system used by KSU. This includes all procedures, equipment, facilities, software, and data used to create, collect, process, store, or transmit information on any university-owned or managed platform.

### **Personally Identifiable Information (PII)**

As defined by KRS 365.732, an individual's first name or first initial and last name, combined with any one or more of the following: Social Security number; driver's license number; or an account, credit, or debit card number in combination with any required security code or password.

## **PROCESS:**

### **Security Program Framework**

KSU will implement and maintain a comprehensive IT security program that addresses, at a minimum, the following areas, which are governed by their own specific policies, regulations, or procedures:

- Acceptable Use
- Awareness and Training
- Access Control
- Audit and Accountability
- Data Classification
- Business Continuity and Disaster Recovery
- Incident Response

### **Incident Reporting Procedure**

Any member of the KSU community who suspects or becomes aware of an Information Security Incident must report the incident immediately through one of the following channels:

- Contact the IT Help Desk or the Chief Information Officer (CIO) directly by phone (preferred), e-mail, or in person.
- Contact their department supervisor, who must then contact the CIO immediately. If the supervisor is unavailable, the individual must contact the appropriate divisional Vice President, who must then contact the CIO immediately.

### **Enforcement**

Any employee, student, or other individual who commits, or refuses to cooperate in the investigation of, a violation of this policy may be subject to disciplinary action, including but not limited to termination, loss of data-access privileges, administrative sanctions, and personal civil and criminal liability.

## **REFERENCES AND RELATED MATERIALS:**

- KSU Appropriate Use of Technology Policy
- KSU Information Technology Audit and Accountability Policy
- KSU Data Classification Policy
- KSU Security and Management Policy
- KRS 365.732

## CONTACTS:

| Subject           | Office            | Telephone      | E-mail   |
|-------------------|-------------------|----------------|--|
| General Questions | Office of the CIO | (502) 597-7000 | <a href="mailto:Wendy.Dixie@kysu.edu">Wendy.Dixie@kysu.edu</a> |

## HISTORY:

| Revision Type                  | Date of Issuance/Revision | Drafter(s)/Editor(s)        |
|--------------------------------|---------------------------|-----------------------------|
| Issued (New Policy)            | April 2020                | Unknown                     |
| Substantive Revisions          | December 18, 2023         | Wendy Dixie and Zach Atwell |
| Minor Revisions (New Template) | June 2025                 | Wendy Dixie and Zach Atwell |

---