PROCEDURE TITLE: SECURITY AWARENESS AND TRAINING

APPLIES TO:

All KSU students, faculty, staff, Board of Regent members, and all others who use, have access to, store, transmit or oversee KSU information technology resources. This applies to access of any KSU information resource from any device.

ADMINISTRATIVE AUTHORITY:

APPROVED BY: Kentucky State University Board of Regents

EFFECTIVE DATE: August 8, 2025

NEXT REVIEW DATE: August 8, 2028

PROCEDURE STATEMENT:

The purpose of this policy is to create and sustain an appropriate level of protection for Information Resources and Systems by improving awareness of information security risks and responsibilities. Specific objectives of this policy include:

1. Increasing awareness to ensure the protection of information resources and systems;
2. Ensuring that users of KSU information technology resources and systems know their roles and responsibilities for protecting information resources and systems;
3. Ensuring that users are knowledgeable about the University's information security policies and practices; and
4. Assisting users with develop skills and knowledge in order to perform their jobs securely

DEFINITIONS:

Cyber Security Threat is any malicious act that tries to obtain access to an information resource or system without authorization.

Security Awareness Training is defined as a method to notify KSU technology users about the importance of protecting information technology resources and systems. Security Awareness Training raining also teaches security key concepts and best practices, such as creating a strong password, following IT Security policies, and reporting security incidents.

PROCESS:

All user of KSU's information resources and systems must have an understanding of the risks associated with using technology and how to effectively defend against cyber threats, both at work and at home. As a result, these users will be required to complete security awareness training which includes knowledge of Kentucky State University's (KSU) information security policies and procedures upon hire and annually thereafter.

In addition to annual training, continuous education such as website information, email messages, and other means will be used. KSU reserves the right to conduct unscheduled awareness assessments to ensure compliance.

ENFORCEMENT

Any individual who violates this policy may result in disciplinary action including but not limited to termination, loss of data access privileges, administrative sanctions, and personal civil and criminal liability.

Any employee or student who interferes with 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 Data Classification Policy
- KSU Data Security Controls Regulation
- KSU Data Access Management Regulation
- KSU Data Backup and Disaster Recovery Regulation

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)	September 2019	Wendy Dixie
Revised (New Template and Substantive Revisions)	June 2025	Zach Atwell