



Kutztown University Policy – GEN-009

Cybersecurity Awareness Policy

A. Purpose

This Cybersecurity Awareness policy provides guidance for the protection of critical data, IT assets, and infrastructures at Kutztown University.

B. Scope

This policy applies to all Information Systems and Information Resources owned or operated by or on behalf of the University. All University-Related Persons with access to University Information or computers and systems operated or maintained on behalf of the University are responsible for adhering to this policy.

C. Definition(s)

Information Resources: University Information and related resources, such as equipment, devices, software, and other information technology.

Security Awareness: Education and communication used to heighten the level of awareness on security topics.

D. Policy

Security Awareness

A security awareness and training program addresses the need for ensuring that security best practices are used when accessing the university's information technology resources. The program promotes active vigilance by training to recognize signs of malicious activity.

A mature security awareness and training program provides adequate resources while actively promoting specific activities within the program. Kutztown University shall establish and maintain the following in support of this program:

Security Awareness and Training Repository

An easy-to-access repository of educational artifacts and references to industry-recognized external resources covering cybersecurity concepts allows employees and students to educate themselves at any time. When possible, resources should avoid heavy technical and legal terms, focusing on layman's terminology for easier adoption of these concepts.

Annual Security Awareness Training

All Kutztown University employees and student workers are expected to complete security awareness training at least once every calendar year. Additional specialized security training may be required for employees based on compliance or access to more sensitive data.

New Hire Training

All University employees, including student employees, with access to Kutztown University Information Resources are expected to complete security awareness training within the first 90 days from date of hire. Annual Security Awareness Training will be completed thereafter.

Email and Web Browser

Email and Web Browsers are vital to the University's operations. They are also the top two most common attack points.

Browser Security

- Only approved web browsers should be used unless specific permission is granted from the KU Office of Information Technology.

Email Security

- University email should not be used to sign up for non-university related sites and services.
- Transferring data via Email or Web must comply with guidelines set forth in the university Data Classification Policy.
- Storing or sending Kutztown University data in personal email is prohibited.

E. Approved By

- Administrative Council – 2/20/25
- President – 3/11/25

F. Effective Date

- 3/11/25