Illinois Wesleyan University
Information Technology Policy

Policy Synopsis

Title: Information Technology Security Training
Approval Date: 01/2025
Revision Date, if applicable: 10/2024
Review Date(s): 01/2026
Related documents: IT Security Procedure

A. Purpose

This policy outlines the Information Technology security training program, and provides the standard process for which training is administered, including completion requirements and steps taken for failure to comply.

Due to the increase in cybersecurity threats and related breaches, it is imperative that the University protects its information as well as the information of all its constituents. Through awareness and training programs, as outlined in this policy, the University will take a proactive stance to ensure data protection and to lessen the risks associated with security incidents. Information Technology Services is committed to supporting the campus community with fulfilling this goal.

B. Policy

1. **Training**

The general training catalog for cybersecurity and regulatory training is available through a self-service portal for all employees and students. In addition, mandatory training will be assigned in three cases:

a. Initial Hire
    i. All new employees of the University are required to complete basic cybersecurity training as part of their onboarding process.
b. Annual Training
    i. Mandatory University-wide training is to be required at least once per year. Notification of the training requirement will be sent to all employees, and at least 30 days will be provided to complete the training.
c. Cybersecurity Incidents
    i. The IT department may assign additional training in situations where there is a clear need for further user training. This includes but is not limited to, security incidents caused by end-user behavior, failure of periodic phishing tests, and situations where additional training is required for specific compliance needs in a given user role (For example, Family Educational Rights and Privacy Act ((FERPA)), training).

2. **Phishing Tests**

As part of the continuous testing of the cybersecurity training program, IT will run periodic phishing tests in which non-malicious content is sent to end users in a manner simulating an actual phishing attempt. Users which erroneously engage with this content may be required to take additional training.

a. Phishing Schedule
    i. Phishing attempts will be launched periodically.
b. Additional Training
    i. If an employee fails a phishing attempt (links are followed, etc.), that employee will be assigned additional training that must be completed under case C above.

3. Enforcement

Completion of assigned training is required by the University, both to ensure compliance with federal and state regulations, and to help protect the Illinois Wesleyan community from malicious actors. In cases of egregious non-compliance, access to specific University IT resources may be temporarily restricted, removed, or denied until training is completed.

Access to certain systems may be dependent on completion of assigned training modules, particularly in cases where these systems store or process sensitive information. For example, access to data covered under FERPA may be restricted until after completion of a FERPA training course.

Specifics of the training enforcement may be found in the IT security training procedures document.