



**Illinois Wesleyan University
Information Technology Policy**

Policy Synopsis

Title: Information Technology Security Training
Approval Date: 08/04/2022
Revision Date, if applicable:
Review Date(s):

A. Purpose

The purpose of this policy is to outline the Information Technology security training that is required in order to maintain Gramm Leach Bliley Act (GLBA) and Illinois State Law 815 compliance. Additionally, this policy provides the standard process by 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 in fulfilling this goal.

B. Compliance Specifications

Gramm-Leach-Bliley Act:

16 CFR 314.4(e) Implement policies and procedures to ensure that personnel are able to enact your information security program by:

(1) Providing your personnel with security awareness training that is updated as necessary to reflect risks identified by the risk assessment;

(2) Utilizing qualified information security personnel employed by you or an affiliate or service provider sufficient to manage your information security risks and to perform or oversee the information security program;

(3) Providing information security personnel with security updates and training sufficient to address relevant security risks; and

(4) Verifying that key information security personnel take steps to maintain current knowledge of changing information security threats and countermeasure

Source: https://www.law.cornell.edu/rio/citation/67_FR_36493

Illinois State Law 815:

(815 ILCS 530/45)

Sec. 45. Data security.

(a) A data collector that owns or licenses, or maintains or stores but does not own or license, records that contain personal information concerning an Illinois resident shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure.

(b) A contract for the disclosure of personal information concerning an Illinois resident that is maintained by a data collector must include a provision requiring the person to whom the information is disclosed to implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure.

(c) If a state or federal law requires a data collector to provide greater protection to records that contain personal information concerning an Illinois resident that are maintained by the data collector and the data collector is in compliance with the provisions of that state or federal law, the data collector shall be deemed to be in compliance with the provisions of this Section.

(d) A data collector that is subject to and in compliance with the standards established pursuant to Section 501(b) of the Gramm-Leach-Bliley Act of 1999, 15 U.S.C. Section 6801, shall be deemed to be in compliance with the provisions of this Section.

(Source: P.A. 99-503, eff. 1-1-17.)

C. Procedures

1. Training

a. Schedule

- i. All Illinois Wesleyan University employees will be required to complete the designated Information Security training two (2) times per year.
 - b. Time to Complete
 - i. All mandatory security training must be completed within forty-five (45) days from the date assigned.
 - ii. Failure to complete within 45 days will result in revocation of access to University systems.
- 2. Phishing
 - a. Phishing Schedule
 - i. Phishing attempts will be launched four (4) times per quarter.
 - b. Additional Training and Non-Compliance
 - i. If an employee fails a phishing attempt (links are followed, etc.), that employee will be assigned additional training that must be completed within thirty (30) days.
 - ii. If training is not completed within 30 days, the employee's supervisor will be notified and an additional fifteen (15) days will be granted to complete the training.
 - iii. If training is not completed within the total allotted time of forty-five (45) days after being assigned, the employee's access to University owned systems will be revoked.