Illinois Wesleyan University
Information Technology Procedure

Procedure Synopsis

Title: Information Technology Security Training Procedure
Approval Date: 01/2025
Revision Date, if applicable: 12/2024
Review Date(s): 01/2026
Related documents: Information Technology Security Training Policy

A. Purpose

This Procedure 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 Procedure, 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. Procedure

1. **Training**

Cybersecurity and compliance training at IWU is provided via KnowBe4, a security training partner. An open catalogue of training modules will be made available to all Faculty, Staff, and Students, but specific modules may be assigned as mandatory training in the following cases:

1. Initial Hire

    a. All new employees of the University are required to complete basic cybersecurity training as part of their onboarding process. The assignment and tracking of these modules is to be managed by the HR department.

2. Annual Training

    a. Mandatory University-wide training will be assigned twice per year, during the Spring and Fall semesters.
    b. Notification of the training requirement will be sent to all employees, and at least 30 days will be provided to complete the training. Selection of the training module(s) to be used will be done by the CISO and the CIO.

3. Cybersecurity Incidents

    a. Additional user training may be assigned by IT in the event of an incident or compromised account being determined to be the result of user negligence. In this case, training tailored to address the incident will be determined by the IT Security team, with approval of the CIO.

2. **Phishing Tests**

Phishing campaigns are to be developed and deployed as needed, with a minimum of once per calendar year.

1. Phishing Schedule

    a. Phishing campaigns will be launched at least once per year, using the KnowBe4 campaign and testing modules. Design of the specific campaign is the responsibility of the IT Security department.

2. Additional Training

    a. 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.

A minimum of 30 days will be given for completion of the training. Training assigned in these instances will be tailored to address the contents of the phishing campaign.

3. Enforcement

Enforcement methods depend upon the type of training assigned.

1. Initial training
    a. In instances where training is a prerequisite for access to a specific system, access to that system will not be granted until training is completed.

2. Annual, Phishing, and Incident Training
    a. Failure to complete assigned training will result in the following set of escalating requests, with each being dependent on the failure of the one before:
        i. Users will receive notifications of remaining time available at least twice before the deadline.
        ii. After the initial deadline, a warning will be sent to the user indicating that training is overdue. An additional week will be provided.
        iii. A notification will be sent to the user as well as the user's supervisor indicating that training is past the deadline, and must be completed within 1 week.
        iv. Notice will be sent to the University CIO for intervention regarding training, and an additional week will be provided.
        v. If the assigned training has not been completed, the user's access to University IT assets and systems will be suspended until completion of the training. It will be necessary for the user to contact the University IT department to restore access, and a window for compliance will be given after reactivation.