Policy Title: IT6009 - Information Technology Security Awareness Training Program

Subject Area: Information Technology

Responsible Official(s): Chief Information Officer

Responsible Office(s): Information Technology Services

Policy Statement

The University of Memphis (UofM) administration takes protecting the University, its intellectual property, financial data, and any personal or confidential information extremely seriously. To help protect these interests and in accordance with the University's Information Security Program (IT6007), an information security awareness training program is provided by the University. This program is intended for select users at the University of Memphis, including, but not limited to, university administration; faculty (including full-time, part-time, adjunct, and emeritus); full-time, part-time, and temporary staff; and student employees.

Definitions

Phishing: the deceptive practice of luring people to reveal personal or confidential information for illicit purposes. Solicitations typically come via telephone, text, websites, or emails.

CIO: Chief Information Officer

CISO: Chief Information Security Officer

Users: All faculty and staff, and the students who have campus jobs that require annual security awareness training.

Policy

All users referenced in the policy statement will be required to complete online training annually. Training modules will be made available during the annual training period, usually the month of October but subject to change as determined by ITS leadership. This training consists of informational modules and videos designed to provide insight and instruction regarding general information security awareness, data privacy, remote working, and related topics.

Training content may vary year-to-year based on current trends. Training may also include relevant policies and guidelines, which employees must acknowledge have been provided.

Additionally, all new employees must complete the online training within one month of their initial hire date. The employee will then be added to the annual training campaign, even if their previous training occurred less than 12 months. In addition to new hire and annual training, the UofM will provide supplemental information on various relevant topics. Training completion and results will be maintained by ITS for each user.

Each user will receive an email from ITS Security when assigned training periods begin and periodically until the training due date. The email will provide all the necessary information to access the training. This is the direct link for the training. Information on Security Awareness Training is also available.

Users referenced in the policy statement may also be included in periodic, simulated phishing campaigns that are designed to reinforce knowledge learned from annual training, as well as other supplemental sources, by simulating a phishing email. Should an individual inappropriately acknowledge or interact with a simulated phishing attack, included but not limited to simulated emails, additional training materials may be assigned to help increase knowledge or close gaps in knowledge to mitigate actual phishing risks.

In accordance with policy IT6003 - Acceptable Use of Information Technology Resources, the CIO, CISO or designee may restrict access to university systems or networks for users who failed to complete the required training by its assigned due date. Access will be returned upon successful completion of the annual security training.

Last Revision Update Log:

IT6009 – Revised February 4, 2026
Originally issued: March 2024