Information Security Awareness Training Program

I. Purpose

The University of North Alabama (UNA) administration takes protecting the University, its intellectual property and any personal or confidential information extremely seriously. To help protect these interests, an information security awareness training program is being provided. This program is intended to set the training standards for all employees at the University of North Alabama, including, but not limited to: university administration; faculty (including full-time, part-time and adjunct); full-time, part-time, and temporary staff; and student employees all of whom are provided service or information by access to university information systems. The success of the University's security awareness training program depends on the ability of all users to work toward a common goal of protecting the University's information and related technical resources.

II. Scope

This program refers to all University information resources whether individually con

administration, research, teaching or other purposes. It is the intent of this program to help users be aw
of actions they can take to better protect the University's information as well as their personal informat
These actions include, but are not limited to: proper password usage, data backup, proper antivirus
protection, reporting any suspected incidents or violations of security policy, and following rules estab
to avoid social engineering attacks.

III. Requirements

All employees referenced in paragraph I above will be required to participate in annual online training (the current cycle occurs during each Spring semester). This training consists of informational videos designed to provide insight and instruction regarding information security. Additionally, all new employees must complete the training within two weeks of their initial hire date. Training may vary year-to-year based on current trends. Failure to complete the annual training is subject to disciplinary actions as defined in the enforcement section of this document. In addition to annual training, UNA will provide supplemental information on various relevant topics. Training completion and results will be maintained for each employee. Finally, the individuals referenced above in paragraph I are included in quarterly phishing campaigns. These campaigns are designed to reinforce knowledge learned from annual training as well as other supplemental sources by producing phishing e-mails. Should an individual inappropriate acknowledge or interact with a phishing test e-mail, additional training materials are supplied to help increase knowledge and close gaps in knowledge to prevent actual phishing success.

IV. Access

Each user will receive an email with a username and temporary password. This email will provide all the necessary information to access the training. The following link can be used to access the training - https://training.knowbe4.com.

V. Enforcement

Any employee who fails to complete the required training will be subject to removal of access to University

For more information regarding security issues, training, concerns, or questions, please contact the Office of Information Technology Services via e-mail at infosec@una.edu, call 256.765.4865 during normal business hours, or visit the ITS department's website at http://www.una.edu/its/technology-security/index.html at any time.