FAYETTEVILLE STATE UNIVERSITY

INFORMATION SECURITY AWARENESS AND TRAINING

Authority:	Issued by the Chancellor. Changes or exceptions to administrative policies issued by the Chancellor may only be made by the Chancellor.
Category:	Information Technology
Applies to:	●Administrators ●Faculty ●Staff
History:	Issued – October 26, 2021
Related Policies/ Regulations/Statutes:	N/A
Contact for Info:	Deputy Chief Information Officer (910) 672-1958

I. PURPOSE

The purpose of this policy (Policy) is to establish information security awareness training requirements for all authorized users of Fayetteville State University's (University) information resources. It is important that all authorized users gain a broad understanding of information security threats, risks, and best practices so as to assist the University in protecting the confidentiality, integrity, and availability of University information resources accessed, managed, and/or controlled by the University.

II. DEFINITIONS

The following definitions are used in this Policy:

- **Availability** shall mean degree to which information and critical College services are accessible for use when required.

- **Confidentiality** shall mean the degree to which confidential University information is protected from unauthorized disclosure.

- **Information Resource** shall mean data, information, and information systems used by the University to conduct University operations. This includes not only the information or data itself, but also computer, network, and storage systems used to interact with the information.

- **Information Security** shall mean the protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional. The focus is on the confidentiality, integrity, and availability of data.

- **Integrity** shall mean the degree to which the accuracy, completeness, and consistency of information is safeguarded to protect the business of the University.

- **Phishing** shall mean the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers**.**

III. TRAINING PROGRAM

The Information Security Office/Officer (ISO) will develop and implement an information security awareness program to be offered periodically to all University authorized users of University information resources.

A. Employee Training

To demonstrate basic competency in information security best practices, University employees must complete this training as part of the onboarding process and annually thereafter, or as required by the ISO. University information resource access privileges may be revoked for authorized users for whom training is required/mandatory who do not complete required/mandatory training within specified timelines. Students will have the option (not the requirement) to complete the information training program.

Training in information security threats and safeguards for University Information Technology Services (IT Services) staff shall be mandatory, with the extent of technical training to reflect the individual's responsibility for configuring and maintaining information security safeguards. Training requirements must be reassessed following any change in job role or responsibilities and new training provided as a priority.

B. Information Security Office/Officer

The ISO shall be responsible for the following:

- Developing or acquiring information security training and test materials.
- Updating and revising training and test materials at least annually to reflect current threats and information security best practices.
- Providing the ability to collect feedback regarding the content and efficacy of the training program.
- Tracking, recording, and reporting training/testing completion rates and other program statistics.
- Ensuring mandatory training compliance across the University.

C. Composition of Training Program

Information security awareness training will include the following:

- Information security awareness best practices.

- Information security roles and responsibilities.
- Acceptable use of University information resources.
- Information classification and handling.
- Causes of unintentional data exposure (e.g. losing a mobile device, emailing the wrong person due to autocomplete)
- Enabling and utilizing security authentication.
- How to identify different forms of social engineering attacks (e.g. phishing, phone scams, impersonation calls).
- Security incident indicators, reporting, and response.
- Security terms and definitions.